Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP2005/022788

International filing date: 12 December 2005 (12.12.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-360436
Filing date: 13 December 2004 (13.12.2004)

Date of receipt at the International Bureau: 30 January 2006 (30.01.2006)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 Date of Application:	２００４年１２月１３日
出 願 番 号 Application Number:	特願２００４－３６０４３６
パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号 The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is	ＪＰ２００４－３６０４３６
出 願 人 Applicant(s):	松下電器産業株式会社 国立大学法人 東京大学

２００６年 １月１１日

特許庁長官
Commissioner,
Japan Patent Office

中嶋 誠

【書類名】　特許願
【整理番号】　2048160371
【提出日】　平成16年12月13日
【あて先】　特許庁長官　殿
【国際特許分類】　G09C　1/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　野仲　真佐男
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　中野　稔久
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　布田　裕一
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　大森　基司
【発明者】
　【住所又は居所】　東京都文京区本郷７－３－１　国立大学法人東京大学内
　【氏名】　五味　剛
【発明者】
　【住所又は居所】　東京都文京区本郷７－３－１　国立大学法人東京大学内
　【氏名】　古原　和邦
【発明者】
　【住所又は居所】　東京都文京区本郷７－３－１　国立大学法人東京大学内
　【氏名】　今井　秀樹
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【特許出願人】
　【識別番号】　504137912
　【氏名又は名称】　国立大学法人東京大学
【代理人】
　【識別番号】　100090446
　【弁理士】
　【氏名又は名称】　中島　司朗
【手数料の表示】
　【予納台帳番号】　014823
　【納付金額】　8,000円
【その他】　国等以外のすべての者の持分の割合１／２
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9003742

【書類名】特許請求の範囲
【請求項１】
利用者端末のクローンを発見するクローン端末発見システムであって、
前記クローン端末発見システムは、前記利用者端末にクローンが存在するか否かを判断する管理センタと、前記利用者端末に関する利用者端末端末情報を前記管理センタへ供給する一以上の情報収集サーバと、前記利用者端末端末情報を前記情報収集サーバへ供給する一以上の前記利用者端末と、から構成され、前記管理センタと前記情報収集サーバは通信路を介して通信可能であって、
前記管理センタは、
管理センタ端末情報を保持する管理センタ記録手段と、
前記情報収集サーバから前記利用者端末端末情報を取得する手段と、
前記管理センタ端末情報及び前記利用者端末端末情報を基に、前記利用者端末にクローンが存在するか否か判断する端末情報確認手段と、
前記端末情報確認手段において、前記利用者端末にクローンが存在するか否かの判断結果を外部へ報知する出力手段と、備え、
前記情報収集サーバは、
可搬媒体を介して、前記利用者端末から前記利用者端末端末情報を収集する情報収集サーバ可搬媒体挿入処理手段と、
通信路を介して、前記前記利用者端末端末情報を前記管理センタへ供給する情報収集サーバ送信処理手段と、を備え、
前記利用者端末は、
前記利用者端末固有の前記利用者端末端末情報を保持する利用者端末記録手段と、
前記可搬媒体を介して、前記利用者端末端末情報を前記情報収集サーバへ供給する可搬媒体データ書込手段と、
を備えることを特徴とする、クローン端末発見システム。
【請求項２】
前記管理センタは、さらに、
前記利用者端末端末情報とは異なる前記第二利用者端末端末情報を生成する端末情報生成手段と、
前記通信路を介して、前記第二利用者端末端末情報を前記情報収集サーバへ供給する管理センタ送信手段、とを備え、
前記情報収集サーバは、さらに、
前記通信路を介して、前記管理センタから前記第二利用者端末端末情報を取得する情報収集サーバ受信手段と、
前記可搬媒体を介して、前記第二利用者端末端末情報を前記利用者端末へ供給する可搬媒体データ書込手段と、を備え、
前記利用者端末は、さらに、
前記可搬媒体を介して、前記第二利用者端末端末情報を前記情報収集サーバから取得する
利用者端末可搬媒体挿入処理手段と、
前記第二利用者端末端末情報を基に、前記利用者端末端末情報を更新する端末情報更新手段と、を備えることを特徴とする、請求項１記載のクローン端末発見システム。
【請求項３】
前記端末情報生成手段は、前記情報収集サーバから前記利用者端末端末情報を取得する毎に、前記第二利用者端末端末情報を生成すること、
を特徴とする請求項２記載のクローン端末発見システム。
【請求項４】
前記端末情報生成手段は、前記情報収集サーバから前記利用者端末端末情報を取得した回数が予め与えられる数を超えた場合、もしくは、予め指定される期間中に１回のみ、前記第二利用者端末端末情報を生成すること、

を特徴とする請求項２記載のクローン端末発見システム。
【請求項５】
前記利用者端末端末情報、及び、前記管理センタ端末情報、及び、前記第二利用者端末端末情報のそれぞれは、前記利用者端末を一意に特定する利用者端末識別子と前記管理センタが生成した乱数を含み、
前記端末情報生成手段で作成される前記第二利用者端末端末情報は、前記利用者端末端末情報に含まれる前記利用者端末識別子と同じ前記利用者端末識別子を含み、前記利用者端末端末情報に含まれる前記乱数とは異なる乱数を含むこと、
を特徴とする請求項２から請求項４に記載のクローン端末発見システム。
【請求項６】
前記端末情報確認手段は、前記管理センタ端末情報に含まれる乱数と前記利用者端末端末情報に含まれる乱数が異なる場合に、前記利用者端末にクローンが存在すると判断することを、
を特徴とする請求項５に記載のクローン端末発見システム。
【請求項７】
前記管理センタ記録手段は、さらに、一以上のタイトル鍵を保持し、
前記管理センタ送信手段は、さらに、何れかの前記タイトル鍵を前記情報収集サーバへ供給し、
前記情報収集サーバ受信手段は、さらに、前記管理センタから前記タイトル鍵を取得し、
前記可搬媒体データ書込手段は、さらに、前記タイトル鍵を前記利用者端末へ供給し、
前記利用者端末可搬媒体挿入処理手段は、さらに、前記タイトル鍵を前記情報収集サーバから取得し、
前記利用者端末は、さらに、
前記タイトル鍵を基にコンテンツが暗号化された暗号化コンテンツを保持する手段と、
前記タイトル鍵を基に、前記暗号化コンテンツを復号化して、前記コンテンツを取得するデスクランブル処理手段と、
前記コンテンツを逐次外部へ出力する出力手段と、
を備えることを特徴とする、請求項２から請求項６に記載のクローン端末発見システム。
【請求項８】
前記管理センタ記録手段は、さらに、前記利用者端末と予め共有している前記利用者端末固有の個別鍵と、一以上のタイトル鍵を保持し、
前記管理センタは、さらに、
前記個別鍵を基に前記タイトル鍵を暗号化し、暗号化タイトル鍵を生成する暗号化タイトル鍵生成手段と、を備え、
前記管理センタ送信手段は、さらに、前記暗号化タイトル鍵を前記情報収集サーバへ供給し、
前記情報収集サーバ受信手段は、さらに、前記管理センタから前記暗号化タイトル鍵を取得し、
前記可搬媒体データ書込手段は、さらに、前記暗号化タイトル鍵を前記利用者端末へ供給し、
前記利用者端末可搬媒体挿入処理手段は、さらに、前記暗号化タイトル鍵を前記情報収集サーバから取得し、
前記利用者端末記録手段は、さらに、前記個別鍵を保持し、
前記利用者端末は、さらに、
前記タイトル鍵を基にコンテンツが暗号化された暗号化コンテンツを保持する手段と、
前記個別鍵を基に前記暗号化タイトル鍵の復号化を行い、前記タイトル鍵を取得する

暗号化タイトル鍵復号化手段と、
　前記タイトル鍵を基に、前記暗号化コンテンツを復号化して、前記コンテンツを取得するデスクランブル処理手段と、
　前記コンテンツを逐次外部へ出力する出力手段と、
を備えることを特徴とする請求項２から請求項６に記載のクローン端末発見システム。
【請求項９】
第一可搬媒体に前記暗号化コンテンツが記録されており、
前記利用者端末は、さらに、
　前記第一可搬媒体から前記暗号化コンテンツを取得する第一可搬媒体アクセス手段と、
を備えることを特徴とする請求項７から請求項８に記載のクローン端末発見システム。
【請求項１０】
利用者端末にクローンが存在するか否か判断する管理センタであって、
前記管理センタは、前記利用者端末に関する利用者端末端末情報を前記管理センタへ供給する一以上の情報収集サーバと通信路を介して通信可能であって、前記収集サーバと前記利用者端末は、可搬媒体を介して通信可能であって、
前記管理センタは、
　管理センタ端末情報を保持する管理センタ記録手段と、
　前記情報収集サーバから前記利用者端末端末情報を取得する手段と、
　前記管理センタ端末情報及び前記利用者端末端末情報を基に、前記利用者端末にクローンが存在するか否か判断する端末情報確認手段と、
　前記端末情報確認手段において、前記利用者端末にクローンが存在するか否かの判断結果を外部へ報知する出力手段と、
を備えることを特徴とする、管理センタ。
【請求項１１】
前記管理センタは、さらに、
　前記利用者端末端末情報とは異なる前記第二利用者端末端末情報を生成する端末情報生成手段と、
　前記通信路を介して、前記第二利用者端末端末情報を前記情報収集サーバへ供給する管理センタ送信手段と、
を備えることを特徴とする、請求項１０記載の管理センタ。
【請求項１２】
前記端末情報生成手段は、前記情報収集サーバから前記利用者端末端末情報を取得する毎に、前記第二利用者端末端末情報を生成すること、
を特徴とする請求項１１記載の管理センタ。
【請求項１３】
前記端末情報生成手段は、前記情報収集サーバから前記利用者端末端末情報を取得した回数が予め与えられる数を超えた場合、もしくは、予め与えられる期間中に１回のみ、前記第二利用者端末端末情報を生成すること、
を特徴とする請求項１１記載の管理センタ。
【請求項１４】
前記利用者端末端末情報、及び、前記管理センタ端末情報、及び、前記第二利用者端末端末情報のそれぞれは、前記利用者端末を一意に識別可能な利用者端末識別子と前記管理センタが生成した乱数を含み、
前記端末情報生成手段で作成される前記第二利用者端末端末情報は、前記利用者端末端末情報に含まれる前記利用者端末識別子と同じ前記利用者端末識別子を含み、前記利用者端末端末情報に含まれる前記乱数とは異なる乱数を含むこと、
を特徴とする請求項１１から請求項１３に記載の管理センタ。
【請求項１５】
前記端末情報確認手段は、前記管理センタ端末情報に含まれる乱数と前記利用者端末端

末情報に含まれる乱数が異なる場合に、前記利用者端末にクローンが存在すると判断すること、
を特徴とする請求項１４に記載の管理センタ。
【請求項１６】
前記管理センタ記録手段は、さらに、一以上のタイトル鍵を保持し、
前記管理センタ送信手段は、さらに、何れかの前記タイトル鍵を前記情報収集サーバへ供給すること、
を特徴とする請求項１１から請求項１５に記載の管理センタ。
【請求項１７】
前記管理センタ記録手段は、さらに、前記利用者端末と予め共有している一以上の前記利用者端末固有の個別鍵と、一以上のタイトル鍵を保持し、
前記管理センタは、さらに、
前記個別鍵を基に前記タイトル鍵を暗号化し、暗号化タイトル鍵を生成する暗号化タイトル鍵生成手段と、を備え、
前記管理センタ送信手段は、さらに、前記暗号化タイトル鍵を前記情報収集サーバへ供給すること、
を特徴とする請求項１１から請求項１６に記載の管理センタ。
【請求項１８】
利用者端末に関する利用者端末端末情報を管理センタへ供給する情報収集サーバであって、
前記情報収集サーバは、前記利用者端末にクローンが存在するか否か判断する管理センタと通信路を介して通信可能であって、さらに、前記利用者端末と可搬媒体を介して通信可能であって、
前記情報収集サーバは、
前記可搬媒体を介して、前記利用者端末から前記利用者端末端末情報を収集する情報収集サーバ可搬媒体挿入処理手段と、
前記通信路を介して、前記前記利用者端末端末情報を前記管理センタへ供給する情報収集サーバ送信処理手段と、
を備えることを特徴とする、情報収集サーバ。
【請求項１９】
利用者端末固有の利用者端末端末情報を情報収集サーバへ供給する利用者端末であって、
前記利用者端末は、前記利用者端末端末情報を前記管理センタへ供給する一以上の情報収集サーバと可搬媒体を介して通信可能であって、さらに、前記利用者端末にクローンが存在するか否か判断する管理センタと前記情報収集サーバは通信路を介して通信可能であって、
前記利用者端末は、
前記利用者端末端末情報を保持する利用者端末記録手段と、
前記可搬媒体を介して、前記利用者端末端末情報を前記情報収集サーバへ供給する可搬媒体データ書込手段と、
を備えることを特徴とする、利用者端末。
【請求項２０】
前記利用者端末は、さらに、
前記可搬媒体を介して、前記第二利用者端末端末情報を前記情報収集サーバから取得する利用者端末可搬媒体挿入処理手段と、
前記第二利用者端末端末情報を基に、保持する前記利用者端末端末情報を更新する端末情報更新手段と
、を備えることを特徴とする、請求項１９記載の利用者端末。
【請求項２１】
前記利用者端末可搬媒体挿入処理手段は、さらに、前記タイトル鍵を前記情報収集サー

バから取得し、
前記利用者端末は、さらに、
前記タイトル鍵を基にコンテンツが暗号化された暗号化コンテンツを保持する手段と、
前記タイトル鍵を基に前記暗号化コンテンツを復号化して、前記コンテンツを取得するデスクランブル処理手段と、
前記コンテンツを逐次外部へ出力する出力手段と、
を備えることを特徴とする、請求項１９から請求項２０に記載の利用者端末。
【請求項２２】
前記利用者端末可搬媒体挿入処理手段は、さらに、前記暗号化タイトル鍵を前記情報収集サーバから取得し、
前記利用者端末記録手段は、さらに、前記利用者端末固有の個別鍵を保持し、
前記利用者端末は、さらに、
前記タイトル鍵を基にコンテンツが暗号化された暗号化コンテンツを保持する手段と、
前記個別鍵を基に前記暗号化タイトル鍵の復号化を行い、前記タイトル鍵を取得する暗号化タイトル鍵復号化手段と、
前記タイトル鍵を基に前記暗号化コンテンツを復号化して、前記コンテンツを取得するデスクランブル処理手段と、
前記コンテンツを逐次外部へ出力する出力手段と、
を備えることを特徴とする、請求項１９から請求項２０に記載の利用者端末。
【請求項２３】
第一可搬媒体に前記暗号化コンテンツが記録されており、
前記利用者端末は、さらに、
前記第一可搬媒体から前記暗号化コンテンツを取得する第一可搬媒体アクセス手段と、
を備えることを特徴とする、請求項２１から請求項２２に記載の利用者端末。
【請求項２４】
利用者端末のクローンが存在するか否かを判断することを目的に、利用者端末端末情報を情報収集サーバへ供給する情報供給方法であって、
前記情報収集方法は、
固有の前記利用者端末端末情報を保持するステップと、
可搬媒体を介して、前記利用者端末端末情報を前記情報収集サーバへ供給するステップと、
を備えることを特徴とする、情報供給方法。
【請求項２５】
前記情報供給方法は、さらに、
前記可搬媒体を介して、前記第二利用者端末端末情報を前記情報収集サーバから取得するステップと、
前記第二利用者端末端末情報を基に、保持する前記利用者端末端末情報を更新するステップと、
を備えることを特徴とする、請求項２４記載の情報供給方法。
【請求項２６】
利用者プログラムのクローンが存在するか否かを判断することを目的に、利用者端末端末情報を情報収集サーバへ供給する利用者プログラムであって、
前記利用者プログラムは、前記利用者プログラムに関する利用者プログラム情報を前記管理センタへ供給する一以上の情報収集サーバと可搬媒体を介して通信可能であって、前記利用者プログラムにクローンが存在するか否か判断する管理センタと前記情報収集サーバは通信路を介して通信可能であって、
前記利用者プログラムは、

前記利用者プログラム固有の前記利用者プログラム情報を保持するステップと、
前記可搬媒体を介して、前記利用者プログラム情報を前記情報収集サーバへ供給するステップと、
を備えることを特徴とする、利用者プログラム。
【請求項２７】
前記利用者プログラムは、さらに、
前記可搬媒体を介して、前記第二利用者プログラム情報を前記情報収集サーバから取得するステップと、
前記第二利用者プログラム情報を基に、保持する前記利用者プログラム情報を更新するステップと、
を備えることを特徴とする、請求項２６記載の利用者プログラム。
【請求項２８】
請求項２６に記載のプログラムを記録した媒体。
【請求項２９】
請求項２７に記載のプログラムを記録した媒体。
【請求項３０】
利用者端末のクローンが存在するか否かを判断することを目的に、利用者端末端末情報を情報収集サーバへ供給する利用者端末の集積回路であって、
前記利用者端末は、前記利用者端末端末情報を前記管理センタへ供給する一以上の情報収集サーバと可搬媒体を介して通信可能であって、さらに、前記利用者端末にクローンが存在するか否か判断する管理センタと前記情報収集サーバは通信路を介して通信可能であって、
前記集積回路は、
前記利用者端末固有の前記利用者端末端末情報を保持する利用者端末記録手段を備え、
前記利用者端末は、
前記可搬媒体を介して、前記利用者端末端末情報を前記情報収集サーバへ供給する可搬媒体データ書込手段と、
を備えることを特徴とする、集積回路。

【書類名】明細書
【発明の名称】クローン端末発見方法
【技術分野】
【０００１】
本発明は、映画や音楽などの著作物であるコンテンツのデジタル化データを再生するシステムに関し、特にクローン端末を利用したコンテンツの再生による著作権侵害を防止するために、クローン端末を発見、あるいは特定するクローン端末発見システムに関する。
【背景技術】
【０００２】
近年、マルチメディア関連技術の発展、大容量記録媒体の出現等を背景として、動画、音声等からからなるデジタルコンテンツ（以下、コンテンツ）を生成して、光ディスク等の大容量記録媒体に格納して配布する、あるいはネットワークや放送を介して配信するシステムが登場している。
一般的に、コンテンツの著作権を保護するため、即ちコンテンツの不正再生や不正コピーといった不正利用を防止するために暗号化技術が用いられる。
【０００３】
具体的には、コンテンツをある暗号化鍵を用いて暗号化して光ディスク等の記録媒体に記録して配布する。これに対して、その暗号化鍵に対応する復号鍵を保有する端末のみが、記録媒体から読み出したデータをその復号鍵を用いて復号して、コンテンツの再生等を行うことができる、というものである。なお、コンテンツを暗号化して記録媒体に記録する方法としては、端末が保有する復号鍵に対応する暗号化鍵でコンテンツそのものを暗号化して記録する方法や、コンテンツをある鍵で暗号化して記録した上で、その鍵に対応する復号用の鍵を、端末が保有する復号鍵に対応する暗号化鍵で暗号化して記録する方法等がある。
【０００４】
このとき、端末が保有する復号鍵は外部に露見しないように厳重に管理される必要があるが、不正者による端末内部の解析において、ある鍵が外部に暴露される危険性がある。ある鍵が一旦不正者に暴露されてしまうと、コンテンツを不正利用する記録装置、再生装置、あるいはソフトウェアを作成して、インターネット等によりそれらを流布することが考えられる。このような場合、著作権者は一旦暴露された鍵では、次から提供するコンテンツを扱えないようにしたいと考える。これを鍵無効化技術と呼び、鍵無効化を実現するシステムとして、特許文献１、あるいは特許文献２が開示されている。
【特許文献１】特開２０００－３１９２２号公報
【特許文献２】特開２００２－２８１０１３号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、前記鍵無効化技術が開示されている特許文献においては、外部に漏れた鍵（無効化すべき鍵）を特定する方法については開示されておらず、特定するためには、市場に大量流通したクローン端末／不正ソフトウェアを回収して、内部を解析することでしか特定できないという課題を有していた。
本発明は、前記課題を解決するもので、可搬媒体を利用して、効率的に無効化すべき鍵を発見、あるいは特定することが可能なクローン端末発見システムを提供することを目的とする。
【課題を解決するための手段】
【０００６】
前記従来の課題を解決するために、本発明のクローン端末発見システムは、利用者端末のクローンを発見するクローン端末発見システムであって、利用者端末にクローンが存在するか否かを判断する管理センタと、利用者端末に関する利用者端末端末情報を管理センタへ供給する一以上の情報収集サーバと、利用者端末端末情報を情報収集サーバへ供給す

る一以上の前記利用者端末と、から構成され、管理センタと情報収集サーバは通信路を介して通信可能であって、管理センタは、管理センタ端末情報を保持する管理センタ記録手段と、情報収集サーバから利用者端末端末情報を取得する手段と、管理センタ端末情報及び利用者端末端末情報を基に、利用者端末にクローンが存在するか否か判断する端末情報確認手段と、端末情報確認手段において、利用者端末にクローンが存在するか否かの判断結果を外部へ報知する出力手段と、備え、情報収集サーバは、可搬媒体を介して、利用者端末から利用者端末端末情報を収集する情報収集サーバ可搬媒体挿入処理手段と、通信路を介して、利用者端末端末情報を管理センタへ供給する情報収集サーバ送信処理手段と、を備え、利用者端末は、利用者端末固有の利用者端末端末情報を保持する利用者端末記録手段と、可搬媒体を介して、利用者端末端末情報を情報収集サーバへ供給する可搬媒体データ書込手段とを有し、効率的に無効化すべき鍵を発見することができる。

【発明の効果】

【０００７】

本発明によれば、効率的に無効化すべき鍵を発見、あるいは特定することが可能である。

【発明を実施するための最良の形態】

【０００８】

以下本発明に係るクローン端末発見システムの実施の形態について、図面を参照しながら説明する。

（実施の形態１）

本発明に係る第１の実施の形態としてのクローン端末発見システム１について説明する。最初に、図１を用いて本実施形態の概要を説明する。

【０００９】

クローン端末発見システム１は、通信路１と管理センタ２と一以上の情報収集サーバ３と一以上の第一可搬媒体４と複数の第二可搬媒体５ａ～５ｍと複数の利用者端末６ａ～６ｎとから構成される。なお、図１では、情報収集サーバ３と第一可搬媒体４と第二可搬媒体５ａと利用者端末６ａを一つずつのみ示している。通信路１は、管理センタ２と情報収集サーバ３とが接続されている通信路であり、インターネット等のネットワークである。管理センタ２は、一以上の情報収集サーバ３から第二可搬媒体５ａ～５ｍの何れかを介して利用者端末６ａ～６ｎの何れかに関する端末情報を受け取り、利用者端末６ａ～６ｎにクローンが存在するか否か判断する。ここでのクローンの定義は、利用者端末毎に個別に与えられている個別鍵を二台以上の利用者端末が保持している状態であるとする。情報収集サーバ３は、例えば動画コンテンツが記録された光ディスクを販売する小売店に設置され、第二可搬媒体５ａ～５ｍに記録されているデータの読み書きが可能な端末であり、第二可搬媒体５ａ～５ｍのいずれかが挿入された場合に、以前その第二可搬媒体が挿入されたことのある利用者端末に関する端末情報を管理センタ２へ送信する。第一可搬媒体４は、例えば動画コンテンツが記録されている光ディスク（例えばＤＶＤ－ＲＯＭ）である。第二可搬媒体５ａ～５ｍはそれぞれ、データの書き換えが可能なポータブルメディア（例えばＳＤカード）である。利用者端末６ａ～６ｎはそれぞれ、第一可搬媒体４に記録されているデータの読み取り、及び第二可搬媒体５ａ～５ｍに記録されているデータの読み書きが可能な端末であり、第一可搬媒体４に記録されているコンテンツを外部へ出力する。ここで、管理センタ２と利用者端末６ａ～６ｎの全ての組には、予め各組が共有している利用者端末識別子と個別鍵と乱数が与えられているとし、例えば管理センタ２と利用者端末６ａは利用者端末識別子ＴＭＩＤａと個別鍵ＩＫａと乱数（管理センタ２が保持する乱数を第一管理センタ乱数ＣＲＮＤ１ａとし、利用者端末６ａが保持する乱数を第一利用者端末乱数ＴＭＲＮＤ１ａと呼ぶ）を、管理センタ２と利用者端末６ｂは利用者端末識別子ＴＭＩＤｂと個別鍵ＩＫｂと乱数（管理センタ２が保持する乱数を第一管理センタ乱数ＣＲＮＤ１ｂとし、利用者端末６ｂが保持する乱数を第一利用者端末乱数ＴＭＲＮＤ１ｂと呼ぶ）を、・・・、管理センタ１１と利用者端末６ｎは利用者端末識別子ＴＭＩＤｎと個別鍵ＩＫｎと乱数（管理センタ２が保持する乱数を第一管理センタ乱数ＣＲＮＤｎとし、

利用者端末６ｎが保持する乱数を第一利用者端末乱数ＴＭＲＮＤｎと呼ぶ）を予め共有しているとする。

【００１０】

ここでは、管理センタ２と情報収集サーバ３と利用者端末６ａ～６ｎの動作について、具体例を交えてもう少し詳細に説明する。一例として、利用者端末６ａを保有するユーザが、動画コンテンツの入ったある光ディスクを小売店で購入して、利用者端末６ａで再生するまでの動作について説明する。ここでは、そのユーザは第二可搬媒体５ａを保持しているとする。

【００１１】

まず事前設定として、ユーザは第二可搬媒体５ａを利用者端末６ａへ挿入し、その際利用者端末６ａは端末情報として、利用者端末識別子ＴＭＩＤａと現在保持している第一利用者端末乱数ＴＭＲＮＤ１ａを第二可搬媒体５ａへ記録する。

そして、ユーザは小売店へ移動し、コンテンツの記録された第一可搬媒体４（光ディスク）を購入する。その第一可搬媒体４には、コンテンツがコンテンツタイトルに対応するタイトル鍵ＴＬＫで暗号化されて記録されているとする。その後、ユーザは小売店に設置されている情報収集サーバ３に可搬媒体５ａを挿入し、ユーザ（もしくは店員）は第一可搬媒体４に記録されているコンテンツのタイトルを識別するタイトル識別子ＴＬＩＤを入力する。そして、情報収集サーバ３は、第二可搬媒体５ａに記録されている端末情報である利用者端末識別子ＴＭＩＤａと第一利用者端末乱数ＴＭＲＮＤ１ａを取得し、入力されたタイトル識別子ＴＬＩＤと共に管理センタ２へ送信する。端末情報である利用者端末識別子ＴＭＩＤａと第一利用者端末乱数ＴＭＲＮＤ１ａと、タイトル識別子ＴＬＩＤを受け取った管理センタ２は、まず管理センタの保持する利用者端末識別子ＴＭＩＤａに対応する第一管理センタ乱数ＣＲＮＤ１ａと受け取った第一利用者端末乱数ＴＭＲＮＤ１ａが一致するか確認する。ここで値が一致しない場合、利用者端末識別子ＴＭＩＤａに対応する利用者端末６ａがクローンである旨、外部に出力する。値が一致した場合、まず利用者端末識別子ＴＭＩＤａに対応する個別鍵ＩＫａを基に、タイトル識別子ＴＬＩＤに対応するタイトル鍵ＴＬＫを暗号化して、暗号化タイトル鍵ＥＮＣＴＬＫを生成する。次に、新たに乱数を一つ生成して、その乱数を第二管理センタ乱数ＣＲＮＤ２ａと第二利用者端末乱数ＴＭＲＮＤ２ａとする。つまり、第二管理センタ乱数ＣＲＮＤ２ａと第二利用者端末乱数ＴＭＲＮＤ２ａは同じ値となる。そして、情報収集サーバ３へ暗号化タイトル鍵ＴＬＫと第二利用者端末乱数ＴＭＲＮＤ２ａを送付し、第二管理センタ乱数ＣＲＮＤ２ａを格納する。管理センタ２から暗号化タイトル鍵ＥＮＣＴＬＫと第二利用者端末乱数ＴＭＲＮＤ２ａを受け取った情報収集サーバ３は、暗号化タイトル鍵ＴＬＫと第二利用者端末乱数ＴＭＲＮＤ２ａを第二可搬媒体５ａに記録する。

【００１２】

第一可搬媒体を小売店で購入したユーザは、まず利用者端末６ａへ第二可搬媒体５ａを挿入する。利用者端末６ａは、第二可搬媒体５ａから暗号化タイトル鍵ＴＬＫと第二利用者端末乱数ＴＭＲＮＤ２ａを受け取る。まず、暗号化タイトル鍵ＥＮＣＴＬＫを自身の保持する個別鍵ＩＫａを基に復号化し、タイトル鍵ＴＬＫを取得し、利用者端末６ａ内に格納する。次に、利用者端末６ａが保持する第一利用者端末乱数ＴＭＲＮＤ１ａの値を第二利用者端末乱数ＴＭＲＮＤ２ａの値に入れ替える。その後、利用者端末６ａに第一可搬媒体４を挿入し、挿入された第一可搬媒体４に記録されたコンテンツタイトルに対応するタイトル鍵ＴＬＫを基に、記録されている暗号化コンテンツＥＮＣＣＮＴを復号化してコンテンツＣＮＴを取得し、外部へ出力する。

【００１３】

なお、ここで用いる暗号処理は、秘密鍵暗号方式による暗号処理である。秘密鍵暗号方式による暗号処理の一例は、ブロック暗号ＡＥＳである。ＡＥＳについては、公知であるので説明を省略する。

以上が、本実施形態の概要である。以下に、本発明のクローン端末発見システムの一実施形態であるクローン端末発見システム１の詳細について説明を行う。これらの構成要素

について詳細に説明する。

【００１４】

＜クローン端末発見システム１の構成＞

クローン端末発見システム１は、通信路１と管理センタ２と一以上の情報収集サーバ３と一以上の第一可搬媒体４と複数の第二可搬媒体５ａ～５ｍと複数の利用者端末６ａ～６ｎとから構成される。以下に、これらの構成要素について詳細に説明する。まず、通信路１及び第一可搬媒体４及び第二可搬媒体５ａ～５ｍについて述べ、続いて管理センタ２及び情報収集サーバ３及び利用者端末６ａ～６ｎの構成と動作について図を用いて説明する。なお、第二可搬媒体５ａ～５ｍのそれぞれは同じ構成であるので、第二可搬媒体５ａを例に挙げて説明する。また、利用者端末６ａ～６ｎのそれぞれはほぼ同じ構成であるので、はじめに利用者端末６ａを例に挙げて説明し、最後に各利用者端末６ａ～６ｎの違いについて説明する。

【００１５】

＜通信路１の構成＞

通信路は、例えば、インターネット、電話回線や専用線等のようなネットワークである。

＜第一可搬媒体４の構成＞

第一可搬媒体４は、例えば、ＤＶＤ－ＲＯＭやＣＤ－ＲＯＭ等のようなあらかじめ動画データなどが暗号化されて書き込まれている可搬媒体であり、図２に示すように、タイトル識別子ＴＬＩＤと、タイトル識別子ＴＬＩＤに対応するタイトル鍵ＴＬＫを基にコンテンツＣＮＴが暗号化された暗号化コンテンツＥＮＣＣＮＴ＝Ｅｎｃ（ＴＬＫ、ＣＮＴ）が記録されている。なお、Ｅｎｃ（Ｋ、Ｐ）を平文Ｐを暗号化鍵Ｋで暗号化した際の暗号文とし、以後同じ表記を用いる。タイトル識別子ＴＬＩＤは、第一可搬媒体４に蓄積されているコンテンツＣＮＴの内容を一意に特定可能な識別子であり、コンテンツＣＮＴは、利用者端末６ａ～６ｎにおいて外部へ出力可能なフォーマット形式のコンテンツデータである。例えば、タイトル識別子ＴＬＩＤは、コンテンツＣＮＴの映画や曲のタイトル、シリアル番号（１、２、３、・・・）などであって、コンテンツＣＮＴは、ＭＰＥＧ２（Ｍｏｖｉｎｇ　Ｐｉｃｔｕｒｅ　Ｅｘｐｅｒｔ　Ｇｒｏｕｐ）フォーマットによる動画コンテンツデータなどである。

【００１６】

＜第二可搬媒体５ａの構成＞

第二可搬媒体５ａは、例えば、ＳＤカード等のようにデータの読み書きが可能なポータブルメディアであり、以前に第二可搬媒体５ａが挿入されたことのある利用者端末に関する端末情報と、その利用者端末向けの鍵情報であるタイトル識別子と暗号化タイトル鍵の組を保持出来るものである。図３では、利用者端末６ａの端末情報と鍵情報を保持している状態を示している。なお、第二可搬媒体５ａには複数の利用者端末の端末情報を保持していても良いし、一つの利用者端末用の鍵情報として、複数組のタイトル識別子と暗号化タイトル鍵を保持していても良い。暗号化タイトル鍵は、対応する利用者端末が保持する個別鍵を基にタイトル鍵ＴＬＫが暗号化された値である。端末情報は、利用者端末識別子と、利用者端末識別子に対応する第一利用者端末乱数と第二利用者端末乱数と、を含む。利用者端末識別子は、利用者端末６ａ～６ｎそれぞれを一意に特定可能な識別子である。第一利用者端末乱数は、第二可搬媒体５ａが対応する利用者端末に最後に挿入された時点で利用者端末が保持していた乱数であり、第二利用者端末乱数は、利用者端末の保持する乱数を更新するために管理センタ２が書き込む乱数の値である。個別鍵ＩＫａ～ＩＫｎは、利用者端末６ａ～６ｎそれぞれが保持する鍵であり、タイトル鍵ＴＬＫは第一可搬媒体４に記録されるコンテンツＣＮＴを暗号化及び復号化する際に用いられる鍵であり、第一可搬媒体４に記録されるコンテンツタイトル毎に異なる鍵である。例えば、第一利用者端末乱数と第二利用者端末乱数と個別鍵とタイトル鍵は、１２８ビットの自然数である。なお。第二利用者端末乱数及び暗号化タイトル鍵は必ずしも記録されていなくてもよい。

【００１７】
＜管理センタ２の構成＞
管理センタ２は、図４に示すように、管理センタ送受信部２１と管理センタ表示部２２と管理センタ記録部２３と管理センタ制御部２４とから構成される。
（１）管理センタ送受信部２１
管理センタ送受信部２１は、モデム等であって、通信路上の情報収集サーバ３からの送信データを受信したり、情報収集端末３へデータを送信したりする。管理センタ送受信部２１は、通信プロトコルとして、たとえば、ＴＣＰ／ＩＰを用いる。
【００１８】
（２）管理センタ表示部２２
管理センタ表示部２２は、液晶パネルやディスプレイ等であって、管理センタ制御部２４からの指示に応じて、必要な画面を表示する。
（３）管理センタ記録部２３
管理センタ記録部２３は、図５に示すように、予め与えられる利用者端末６ａ～６ｎの端末情報である利用者端末識別子ＴＭＩＤａ～ＴＭＩＤｎと第一管理センタ乱数ＣＲＮＤｌａ～ＣＲＮＤｌｎと個別鍵ＩＫａ～ＩＫｎ、及び、予め与えられるタイトル鍵情報であるタイトル識別子とタイトル鍵ＴＬＫの組を一組以上記録されている。また、各利用者端末識別子ＴＭＩＤａ～ＴＭＩＤｎに対応して、第二管理センタ乱数ＣＲＮＤ２ａ～ＣＲＮＤ２ｎも記録可能である。第一管理センタ乱数は、第二可搬媒体から端末情報を受け取った最後の時点で対応する利用者端末が保持していた乱数であり、第二管理センタ乱数は、利用者端末の保持する乱数を更新するために管理センタ２が以前第二可搬媒体に書き込んだ乱数の値である。なお、第一管理センタ乱数ＣＲＮＤｌａ～ＣＲＮＤｌｎと第二管理センタ乱数ＣＲＮＤ２ａ～ＣＲＮＤ２ｎの値は変更可能である。例えば、第一管理センタ乱数と第二管理センタ乱数は、１２８ビットの自然数である。なお、第二利用者端末乱数は必ずしも記録されていなくてもよい。
【００１９】
（４）管理センタ制御部２４
管理センタ制御部２４は、図４で示すとおり、管理センタ受信処理部２４１と、端末情報確認部２４２と、端末情報生成部２４３と、タイトル鍵暗号化部２４４と、管理センタ送信データ生成部２４５と、管理センタ送信処理部２４６とを含む。管理センタ制御部２４は、各機能部を有する専用のマイクロコンピュータ等である。各機能部は、マイクロコンピュータにマスクされているプログラムによって実現される。なお、各機能部は、独立のマイクロコンピュータであってもよい。
【００２０】
（４－１）管理センタ受信処理部２４１
管理センタ受信処理部２４１は、管理センタ送受信部２１を介して、情報収集サーバ３から利用者端末識別子と第一利用者端末乱数とタイトル識別子を受け取る。そして、受け取った利用者端末識別子と第一利用者端末乱数を端末情報確認部２４２へ出力し、利用者端末識別子とタイトル識別子をタイトル鍵暗号化部２４４へ出力する。
【００２１】
（４－２）端末情報確認部２４２
端末情報確認部２４２は、管理センタ受信処理部２４１から利用者端末識別子と第一利用者端末乱数を取得する。そして、管理センタ記録部２３から、受け取った利用者端末識別子に対応する第一管理センタ乱数を取得する。また、利用者端末識別子に対応する第二管理センタ乱数が記録されている場合、第二管理センタ乱数も取得する。
【００２２】
まず、第二管理センタ乱数が記録されている場合、第一利用者端末乱数と第二管理センタ乱数が一致しているかどうか確認する。そこで、第一利用者端末乱数と第二管理センタ乱数が一致している場合、管理センタ記録部２３に記録されている第一管理センタ乱数の値に第二管理センタ乱数の値をコピーし、第二管理センタ乱数を消去する。そして、端末

情報生成部２４３へ利用者端末識別子を出力し、タイトル鍵暗号化部２４４へ暗号化タイトル鍵生成要求を出力する。次に、第二管理センタ乱数が記録されているが第一利用者端末乱数と第二管理センタ乱数が一致しない場合、もしくは、第二管理センタ乱数が記録されていない場合、第一利用者端末乱数と第一管理センタ乱数が一致しているかどうか確認する。そこで、第一利用者端末乱数と第一管理センタ乱数が一致していない場合、利用者端末識別子に対応する利用者端末がクローンであることを示す画面を管理センタ表示部２２に表示させる。一方、第一利用者端末乱数と第一管理センタ乱数が一致していた場合、端末情報生成部２４３へ利用者端末識別子を出力し、タイトル鍵暗号化部２４４へ暗号化タイトル鍵生成要求を出力する。

【００２３】

（４－３）端末情報生成部２４３

端末情報生成部２４３は、端末情報確認部２４２から利用者端末識別子を取得する。そこでまず乱数を生成する。乱数を生成する方法については公知であるので説明を省略する。そして、その乱数を、管理センタ記録部２３の利用者端末識別子に対応する第二管理センタ乱数として記録する。また、同一の乱数を、第二利用者端末乱数として、管理センタ送信データ生成部２４５へ出力する。

【００２４】

（４－４）タイトル鍵暗号化部２４４

タイトル鍵暗号化部２４４は、管理センタ受信処理部２４１から利用者端末識別子とタイトル識別子を取得する。また、端末情報確認部２４２から暗号化タイトル鍵生成要求を取得する。そして、まず、管理センタ記録部２３から、利用者端末識別子に対応する個別鍵を取得する。また、タイトル識別子に対応するタイトル鍵を取得する。その後、個別鍵を基にタイトル鍵を暗号化して、暗号化タイトル鍵を生成する。最後に、タイトル識別子と暗号化タイトル鍵を管理センタ送信データ生成部２４５へ出力する。

【００２５】

（４－５）管理センタ管理センタ送信データ生成部２４５

管理センタ送信データ生成部２４５は、端末情報生成部２４３から第二利用者端末乱数を取得する。また、タイトル鍵暗号化部２４４からタイトル識別子と暗号化タイトル鍵を取得する。そして、取得した第二利用者端末乱数とタイトル識別子と暗号化タイトル鍵から、情報収集サーバ３へ送付するデータを生成する。そして、その生成したデータを管理センタ送信処理部２４６に出力する。

【００２６】

（４－６）管理センタ管理センタ送信処理部２４６

管理センタ送信処理部２４６は、管理センタ送信データ生成部２４５からデータを取得する。そして、そのデータを管理センタ送受信部２１を介して、情報収集サーバ３へ送信する。

＜管理センタ２の動作＞

以上で、管理センタ２の構成について説明を行ったが、次に管理センタ２の動作についてフローチャートを用いて説明する。ここでは、情報収集サーバ３から利用者端末識別子ＴＭＩＤａと第一利用者端末乱数ＴＭＲＮＤ１ａとタイトル識別子ＴＬＩＤを受け取った場合を例に挙げ、図６を用いて説明する。

【００２７】

管理センタ受信処理部２４１は、情報収集サーバ３から利用者端末識別子ＴＭＩＤａと第一利用者端末乱数ＴＭＲＮＤ１ａとタイトル識別子ＴＬＩＤを受け取り、その利用者端末識別子ＴＭＩＤａと第一利用者端末乱数ＴＭＲＮＤ１ａとを端末情報確認部２４２へ出力し、利用者端末識別子ＴＭＩＤａとタイトル識別子ＴＬＩＤをタイトル鍵暗号化部２４４へ出力する。（Ｓ２０１）

端末情報確認部２４２は、管理センタ受信処理部２４１から利用者端末識別子ＴＭＩＤａと第一利用者端末乱数ＴＭＲＮＤ１ａを取得する。（Ｓ２０２）

管理センタ記録部２３に利用者端末識別子ＴＭＩＤａに対応する第二管理センタ乱数Ｃ

ＲＮＤ２ａが記録されている場合、ステップＳ２０４に進む。一方、利用者端末識別子ＴＭＩＤａに対応する第二管理センタ乱数ＣＲＮＤ２ａが記録されていない場合、ステップＳ２０７に進む。（Ｓ２０３）

端末情報確認部２４２は、管理センタ記録部２３から第二管理センタ乱数ＣＲＮＤ２ａを取得する。（Ｓ２０４）

第一利用者端末乱数ＴＭＲＮＤ１ａの値と第二管理センタ乱数ＣＲＮＤ２ａの値が一致している場合、ステップＳ２０６に進む。一方、第一利用者端末乱数ＴＭＲＮＤ１ａの値と第二管理センタ乱数ＣＲＮＤ２ａの値が一致していない場合、ステップＳ２０７に進む。（Ｓ２０５）

第一管理センタ乱数ＣＲＮＤ１ａの値に第二管理センタ乱数ＣＲＮＤ２ａの値をコピーし、第二管理センタ乱数ＣＲＮＤ２ａを消去する。ステップＳ２１０に進む。（Ｓ２０６）

端末情報確認部２４２は、管理センタ記録部２３から、その利用者端末識別子ＴＭＩＤａに対応する第一管理センタ乱数ＣＲＮＤ１ａを取得する。（Ｓ２０７）

第一利用者端末乱数ＴＭＲＮＤ１ａの値と第一管理センタ乱数ＣＲＮＤ１ａの値が一致している場合、ステップＳ２１０に進む。一方、第一利用者端末乱数ＴＭＲＮＤ１ａの値と第一管理センタ乱数ＣＲＮＤ１ａの値が一致していない場合、ステップＳ２０９に進む。（Ｓ２０８）

端末情報確認部２４２は、利用者端末識別子ＴＭＩＤａに対応する利用者端末がクローンであることを示す画面を管理センタ表示部２２に表示させ、ステップＳ２１０へ進む。例えば、「クローンを発見しました：利用者端末識別子ＴＭＩＤａ」と表示する。ステップＳ２１０へ進む。（Ｓ２０９）

端末情報確認部２４２は、端末情報生成部２４３へ利用者端末識別子ＴＭＩＤａを出力し、タイトル鍵暗号化部２４４へ暗号化タイトル鍵生成要求を出力する。（Ｓ２１０）

端末情報生成部２４３は、端末情報確認部２４２から利用者端末識別子ＴＭＩＤａを取得する。そして、まず乱数を生成する。その乱数を管理センタ記録部２３の利用者端末識別子ＴＭＩＤａに対応する第二管理センタ乱数ＣＲＮＤ２ａの値として記録する。また、同じ乱数を、第二利用者端末乱数ＴＭＲＮＤ２ａとして、管理センタ送信データ生成部２４５へ出力する。（Ｓ２１１）

タイトル鍵暗号化部２４４は、管理センタ受信処理部２４１から利用者端末識別子ＴＭＩＤａとタイトル識別子ＴＬＩＤを取得する。また、端末情報確認部２４２から暗号化タイトル鍵生成要求を取得する。そこでまず、管理センタ記録部２３から、利用者端末識別子ＴＭＩＤａに対応する個別鍵ＩＫａを取得する。また、タイトル識別子ＴＬＩＤに対応するタイトル鍵ＴＬＫを取得する。そして、個別鍵ＩＫａを基にタイトル鍵ＴＬＫを暗号化して、暗号化タイトル鍵ＥＮＣＴＬＫａ＝Ｅｎｃ（ＴＫ、ＩＫａ）を生成する。そして、タイトル識別子ＴＬＩＤと暗号化タイトル鍵ＥＮＣＴＬＫａを管理センタ送信データ生成部２４５へ出力する。（Ｓ２１２）

管理センタ送信データ生成部２４５は、端末情報生成部２４３から第二利用者端末乱数ＴＭＲＮＤ２ａを取得する。また、タイトル鍵暗号化部２４４からタイトル識別子ＴＬＩＤと暗号化タイトル鍵ＥＮＣＴＬＫａを取得する。そして、取得した第二利用者端末乱数ＴＭＲＮＤ２ａとタイトル識別子ＴＬＩＤと暗号化タイトル鍵ＥＮＣＴＬＫａを情報収集サーバ３へ送付する送信データを生成する。そして、その生成した送信データを管理センタ送信処理部２４６に出力する。（Ｓ２１３）

管理センタ送信処理部２４６は、管理センタ送信データ生成部２４５から送信データを取得する。そして、その送信データを管理センタ送受信部２１を介して、情報収集サーバ３へ送信する。終了する。（Ｓ２１４）

以上が、クローン端末発見システム１の構成要素である管理センタ２の構成と動作である。続いて、情報収集サーバ３の構成と動作について説明を行う。

【００２８】

＜情報収集サーバ３の構成＞

情報収集サーバ３は、図７に示すように、情報収集サーバ送受信部３１と可搬媒体アクセス部３２と外部入力部３３と情報収集サーバ制御部３４とから構成される。

（１）情報収集サーバ送受信部３１

情報収集サーバ送受信部３１は、モデム等であって、通信路上の管理センタ２からの情報を受信したり、管理センタ２へ情報を送信したりする。情報収集サーバ送受信部３１は、通信プロトコルとして、たとえば、ＴＣＰ／ＩＰを用いる。

【００２９】

（２）情報収集サーバ第二可搬媒体アクセス部３２

情報収集サーバ第二可搬媒体アクセス部３２は、例えばＳＤカードリーダであって、情報収集サーバ３に第二可搬媒体が挿入されたことを検知したり、挿入されている第二可搬媒体に記録されているデータを取得したり、挿入されている第二可搬媒体にデータを記録したりする。

【００３０】

（３）外部入力部３３

外部入力部３３は、外部からタイトル識別子ＴＬＩＤを入力可能なものであって、例えば数字０～９やアルファベットＡ～Ｚを入力可能なキーボードやキーパット、マウスである。

（４）情報収集サーバ制御部３４

情報収集サーバ制御部３４は、情報収集サーバ第二可搬媒体挿入処理部３４１と、タイトル情報取得部３４２と、送信データ処理部３４３と、情報収集サーバ送信処理部３４４と、情報収集サーバ受信処理部３４５と、第二可搬媒体データ書込部３４６とを含む。情報収集サーバ制御部３４は、各機能部を有する専用のマイクロコンピュータ等である。各機能部は、マイクロコンピュータにマスクされているプログラムによって実現される。なお、各機能部は、独立のマイクロコンピュータであってもよい。

【００３１】

（４－１）情報収集サーバ第二可搬媒体挿入処理部３４１

情報収集サーバ第二可搬媒体挿入処理部３４１は、情報収集サーバ第二可搬媒体アクセス部３２経由で情報収集サーバ３に第二可搬媒体が挿入されたことを検知した場合、情報収集サーバ第二可搬媒体アクセス部３２を介して第二可搬媒体に記録されている利用者端末識別子と第一利用者端末乱数を取得する。そして、受け取った利用者端末識別子と第一利用者端末乱数を情報収集サーバ送信データ生成部３４３へ出力し、タイトル情報要求をタイトル情報取得部３４２へ出力する。

【００３２】

（４－２）タイトル情報取得部３４２

タイトル情報取得部３４２は、情報収集サーバ第二可搬媒体挿入処理部３４１からタイトル情報要求を受け取った場合、外部入力部３３経由で、タイトル識別子を取得する。そして、取得したタイトル識別子を情報収集サーバ送信データ生成部３４３へ出力する。

（４－３）情報収集サーバ送信データ生成部３４３

情報収集サーバ送信データ生成部３４３は、情報収集サーバ第二可搬媒体挿入処理部３４１から利用者端末識別子と第一利用者端末乱数を取得する。また、タイトル情報取得部３４２からタイトル識別子を取得する。そして、取得した利用者端末識別子と第一利用者端末乱数とタイトル識別子とから、管理センタ２へ送付する送信データを生成する。そして、その生成した送信データを情報収集サーバ送信処理部３４４に出力する。

【００３３】

（４－４）情報収集サーバ送信処理部３４４

情報収集サーバ送信処理部３４４は、情報収集サーバ送信データ生成部３４３から送信データを取得する。そして、その送信データを情報収集サーバ送受信部３１を介して、管理センタ２へ送信する。

（４－５）情報収集サーバ受信処理部３４５

情報収集サーバ受信処理部３４５は、情報収集サーバ送受信部３１を介して、管理セン

タ２から第二利用者端末乱数とタイトル識別子と暗号化タイトル鍵を受け取る。そして、受け取った第二利用者端末乱数とタイトル識別子と暗号化タイトル鍵を第二可搬媒体データ書込部３４６へ出力する。

【００３４】

（４－６）第二可搬媒体データ書込部３４６

第二可搬媒体データ書込部３４６は、情報収集サーバ受信処理部３４５から第二利用者端末乱数とタイトル識別子と暗号化タイトル鍵を受け取る。そして、受け取った第二利用者端末乱数とタイトル識別子と暗号化タイトル鍵を情報収集サーバ第二可搬媒体アクセス部３２経由で、第二可搬媒体へ記録する。

【００３５】

＜情報収集サーバ３の動作＞

以上で、情報収集サーバ３の構成について説明を行ったが、次に情報収集サーバ３の動作についてフローチャートを用いて説明する。ここでは、ユーザはタイトル識別子ＴＬＩＤに対応するコンテンツの記録された第一可搬媒体４を購入し、ユーザが第二可搬媒体５ａを保有しているとする。そして、情報収集サーバ３へその第二可搬媒体５ａが挿入された場合を例に挙げ、図８を用いて情報収集サーバ３の動作を説明する。なお、情報収集サーバ３へ第二可搬媒体５ａが挿入される前に、第二可搬媒体５ａはそのユーザの保有する利用者端末６ａへ挿入されていて、利用者端末６ａの端末情報（利用者端末識別子ＴＭＩＤａと第一利用者端末乱数ＴＭＲＮＤ１ａ）を取得しているとする。

【００３６】

情報収集サーバ第二可搬媒体挿入処理部３４１は、情報収集サーバ第二可搬媒体アクセス部３２経由で情報収集サーバ３に第二可搬媒体５ａが挿入されたことを検知する。（Ｓ３０１）

情報収集サーバ第二可搬媒体挿入処理部３４１は、情報収集サーバ第二可搬媒体アクセス部３２を介して第二可搬媒体５ａに記録されている利用者端末識別子ＴＭＩＤａと第一利用者端末乱数ＴＭＲＮＤ１ａを取得する。（Ｓ３０２）

情報収集サーバ第二可搬媒体挿入処理部３４１は、受け取った利用者端末識別子ＴＭＩＤａと第一利用者端末乱数ＴＭＲＮＤ１ａを情報収集サーバ送信データ生成部３４３へ出力し、タイトル情報要求をタイトル情報取得部３４２へ出力する。（Ｓ３０３）

タイトル情報取得部３４２は、情報収集サーバ第二可搬媒体挿入処理部３４１からタイトル情報要求を受け取り、外部入力部３３経由で、タイトル識別子ＴＬＩＤを取得する。（Ｓ３０４）

タイトル情報取得部３４２は、取得したタイトル識別子ＴＬＩＤを情報収集サーバ送信データ生成部３４３へ出力する。（Ｓ３０５）

情報収集サーバ送信データ生成部３４３は、情報収集サーバ第二可搬媒体挿入処理部３４１から利用者端末識別子ＴＭＩＤａと第一利用者端末乱数ＴＭＲＮＤ１ａを取得し、タイトル情報取得部３４２からタイトル識別子ＴＬＩＤを取得する。そして、取得した利用者端末識別子ＴＭＩＤａと第一利用者端末乱数ＴＭＲＮＤ１ａとタイトル識別子ＴＬＩＤから、管理センタ２へ送付する送信データを生成する。そして、生成した送信データを情報収集サーバ送信処理部３４４に出力する。（Ｓ３０６）

情報収集サーバ送信処理部３４４は、情報収集サーバ送信データ生成部３４３から送信データを取得し、その送信データを情報収集サーバ送受信部３１を介して、管理センタ２へ送信する。（Ｓ３０７）

情報収集サーバ受信処理部３４５は、通信路１を介して、管理センタ２から送信データを受信した場合、ステップＳ３０９へ進む。もし受信していない場合、ステップＳ３０８を繰り返す。（Ｓ３０８）

情報収集サーバ受信処理部３４５は、情報収集サーバ送受信部３１を介して、管理センタ２から第二利用者端末乱数ＴＭＲＮＤ２ａとタイトル識別子ＴＬＩＤと暗号化タイトル鍵ＥＮＣＴＬＫａを受け取る。そして、受け取った第二利用者端末乱数ＴＭＲＮＤ２ａとタイトル識別子ＴＬＩＤと暗号化タイトル鍵ＥＮＣＴＬＫａを第二可搬媒体データ書込部

３４６へ出力する。（Ｓ３０９）
第二可搬媒体データ書込部３４６は、情報収集サーバ受信処理部３４５から第二利用者端末乱数ＴＭＲＮＤ２ａとタイトル識別子ＴＬＩＤと暗号化タイトル鍵ＥＮＣＴＬＫａを受け取り、受け取った第二利用者端末乱数ＴＭＲＮＤ２ａとタイトル識別子ＴＬＩＤと暗号化タイトル鍵ＥＮＣＴＬＫａを情報収集サーバ第二可搬媒体アクセス部３２経由で、第二可搬媒体５ａへ記録する。（Ｓ３１０）
以上が、クローン端末発見システム１の構成要素である情報収集サーバ３の構成と動作である。続いて、利用者端末６ａの構成と動作について説明を行う。
【００３７】
＜利用者端末６ａの構成＞
利用者端末６ａは、図９に示すように、利用者端末第二可搬媒体アクセス部６１、第一可搬媒体アクセス部６２、出力部６３、利用者端末記録部６４、利用者端末制御部６５とから構成される。
（１）利用者端末第二可搬媒体アクセス部６１
利用者端末第二可搬媒体アクセス部６１は、例えばＳＤカードリーダであって、利用者端末６ａに第二可搬媒体が挿入されたことを検知したり、挿入されている第二可搬媒体に記録されているデータを取得したり、挿入されている第ニ可搬媒体にデータを記録したりする。
【００３８】
（２）第一可搬媒体アクセス部６２
第一可搬媒体アクセス部６２は、例えばＤＶＤドライブであって、利用者端末６ａに第一可搬媒体が挿入されたことを検知したり、挿入されている第一可搬媒体に記録されているデータを取得したりする。
（３）出力部６３
出力部６３は、例えば外部の液晶ディスプレイやプラズマテレビ等と接続され、利用者端末制御部６５から受け取ったデータを外部へ表示するものである。
【００３９】
（４）利用者端末記録部６４
利用者端末記録部６４は、図１０に示すように、予め与えられる利用者端末６ａに関する端末情報である利用者端末識別子ＴＭＩＤａと第一利用者端末乱数ＴＭＲＮＤ１ａと個別鍵ＩＫａとが記録されている。また、利用者端末記録部６４には、タイトル鍵情報であるタイトル識別子とタイトル鍵の組を複数記録可能である。なお、第一利用者端末乱数ＴＭＲＮＤ１ａの値は変更可能である。また、タイトル識別子とタイトル鍵の組を追記することが可能である。
【００４０】
（５）利用者端末制御部６５
利用者端末制御部６５は、利用者端末第二可搬媒体挿入処理部６５１と、端末情報書込部６５２と、暗号化タイトル鍵復号化部６５３と、端末情報更新部６５４と、第一可搬媒体挿入処理部６５５と、デスクランブル処理部６５６とを含む。利用者端末制御部６５は、各機能部を有する専用のマイクロコンピュータ等である。各機能部は、マイクロコンピュータにマスクされているプログラムによって実現される。なお、各機能部は、独立のマイクロコンピュータであってもよい。
【００４１】
（５－１）利用者端末第二可搬媒体挿入処理部６５１
利用者端末第二可搬媒体挿入処理部６５１は、利用者端末第二可搬媒体アクセス部６１経由で利用者端末６ａに第二可搬媒体が挿入されたことを検知する。そしてまず、利用者端末記録部６４に記録されている利用者端末識別子ＴＭＩＤａを取得する。その次に、利用者端末第二可搬媒体アクセス部６１経由で第二可搬媒体に利用者端末識別子ＴＭＩＤａが記録されているかどうか確認する。ここで、もし第二可搬媒体に利用者端末識別子ＴＭＩＤａが記録されていない場合、端末情報書込部６５２へ利用者端末識別子ＴＭＩＤａを

出力する。一方、第二可搬媒体に利用者端末識別子ＴＭＩＤａが記録されている場合、第二可搬媒体に利用者端末識別子ＴＭＩＤａに対応する第二利用者端末乱数ＴＭＲＮＤ２ａとタイトル識別子ＴＬＩＤと暗号化タイトル鍵ＥＮＣＴＬＫａが記録されているかどうか確認する。ここで、もし第二可搬媒体に利用者端末識別子ＴＭＩＤａに対応する第二利用者端末乱数ＴＭＲＮＤ２ａと暗号化タイトル鍵ＥＮＣＴＬＫａが記録されている場合、第二利用者端末乱数ＴＭＲＮＤ２ａを端末情報更新部６５４へ出力し、タイトル識別子ＴＬＩＤと暗号化タイトル鍵ＥＮＣＴＬＫａを暗号化タイトル鍵復号化部６５３へ出力する。そして、第二利用者端末乱数ＴＭＲＮＤ２ａの値を第一利用者端末乱数ＴＭＲＮＤ１ａの値として、利用者端末識別子ＴＭＩＤａに対応付けて第二可搬媒体に記録する。

【００４２】

（５－２）端末情報書込部６５２

端末情報書込部６５２は、利用者端末第二可搬媒体挿入処理部６５１から利用者端末識別子ＴＭＩＤａを取得する。その後、利用者端末記録部６４に記録されている第一利用者端末乱数を取得し、利用者端末識別子ＴＭＩＤａと第一利用者端末乱数ＴＭＲＮＤ１ａを第二可搬媒体に記録する。

【００４３】

（５－３）暗号化タイトル鍵復号化部６５３

暗号化タイトル鍵復号化部６５３は、利用者端末第二可搬媒体挿入処理部６５１からタイトル識別子ＴＬＩＤと暗号化タイトル鍵ＥＮＣＴＬＫａを取得する。そして、利用者端末記録部６４から個別鍵ＩＫａを取得する。その次に、個別鍵ＩＫａを基に暗号化タイトル鍵ＥＮＣＴＬＫａの復号化を行い、タイトル鍵ＴＬＫを取得する。最後に、タイトル識別子ＴＬＩＤとそのタイトル鍵ＴＬＫを利用者端末記録部６４へ新たに記録する。

【００４４】

（５－４）端末情報更新部６５４

端末情報更新部６５４は、利用者端末第二可搬媒体挿入処理部６５１から第二利用者端末乱数ＴＭＲＮＤ２ａを取得する。そして、利用者端末記録部６４に記録されている第一利用者端末乱数ＴＭＲＮＤ１ａの値を、第二利用者端末乱数ＴＭＲＮＤ２ａの値に変更する。

【００４５】

（５－５）第一可搬媒体挿入処理部６５５

第一可搬媒体挿入処理部６５５は、第一可搬媒体アクセス部６２経由で利用者端末６ａに第一可搬媒体４が挿入されたことを検知する。そしてまず、第一可搬媒体アクセス部６２経由で第一可搬媒体４に記録されているタイトル識別子ＴＬＩＤを取得する。そして、タイトル識別子ＴＬＩＤに対応するタイトル鍵ＴＬＫが利用者端末記録部６４に記録されているかどうか確認する。もしタイトル識別子ＴＬＩＤに対応するタイトル鍵ＴＬＫが記録されている場合、利用者端末記録部６４からタイトル鍵ＴＬＫを取得し、デスクランブル処理部６５６へ出力する。

【００４６】

（５－６）デスクランブル処理部６５６

デスクランブル処理部６５６は、第一可搬媒体挿入処理部６５５からタイトル鍵ＴＬＫを取得する。その後、第一可搬媒体アクセス部６２経由で第一可搬媒体４に記録されている暗号化コンテンツを逐次取得し、タイトル鍵ＴＬＫを基に暗号化コンテンツを逐次でスクランブルを行い、出力部６３経由で外部へ逐次出力する。

【００４７】

＜利用者端末６ａの動作＞

以上で、利用者端末６ａの構成について説明を行ったが、次に利用者端末６ａの動作について説明する。まず、利用者端末６ａへ第二可搬媒体５ａを挿入した場合の動作について図１１に示すフローチャートを用いて説明する。続いて、利用者端末６ａへ第一可搬媒体４を挿入した場合の動作について図１２に示すフローチャートを用いて説明する。

【００４８】

＜利用者端末６ａへ第二可搬媒体５ａを挿入した場合の動作＞
利用者端末第二可搬媒体挿入処理部６５１は、利用者端末第二可搬媒体アクセス部６１経由で利用者端末６ａに第二可搬媒体５ａが挿入されたことを検知する。そしてまず、利用者端末記録部６４に記録されている利用者端末識別子ＴＭＩＤａを取得する。（Ｓ６０１）
第二可搬媒体５ａに利用者端末識別子ＴＭＩＤａが記録されている場合、ステップＳ６０４に進む。一方、第二可搬媒体５ａに利用者端末識別子ＴＭＩＤａが記録されていない場合、ステップＳ６０３に進む。（Ｓ６０２）
端末情報書込部６５２へ利用者端末識別子ＴＭＩＤａを出力する。端末情報書込部６５２は、利用者端末第二可搬媒体挿入処理部６５１から利用者端末識別子ＴＭＩＤａを取得する。その後、利用者端末記録部６４に記録されている第一利用者端末乱数を取得し、利用者端末識別子ＴＭＩＤａと第一利用者端末乱数ＴＭＲＮＤ１ａを第二可搬媒体５ａに記録する。終了する。（Ｓ６０３）
第二可搬媒体５ａに利用者端末識別子ＴＭＩＤａに対応する第二利用者端末乱数ＴＭＲＮＤ２ａが記録されている場合、ステップＳ６０５に進む。第二可搬媒体５ａに利用者端末識別子ＴＭＩＤａに対応する第二利用者端末乱数ＴＭＲＮＤ２ａが記録されていない場合、ステップＳ６０６に進む。（Ｓ６０４）
第二利用者端末乱数ＴＭＲＮＤ２ａを端末情報更新部６５４へ出力する。端末情報更新部６５４は、利用者端末第二可搬媒体挿入処理部６５１から第二利用者端末乱数ＴＭＲＮＤ２ａを取得する。そして、利用者端末記録部６４に記録されている第一利用者端末乱数ＴＭＲＮＤ１ａの値を、第二利用者端末乱数ＴＭＲＮＤ２ａの値に変更する。（Ｓ６０５）
第二可搬媒体５ａに利用者端末識別子ＴＭＩＤａに対応するタイトル識別子ＴＬＩＤと暗号化タイトル鍵ＥＮＣＴＬＫａが記録されている場合、ステップＳ６０７に進む。第二可搬媒体５ａに利用者端末識別子ＴＭＩＤａに対応するタイトル識別子ＴＬＩＤと暗号化タイトル鍵ＥＮＣＴＬＫａが記録されていない場合、終了する。（Ｓ６０６）
暗号化タイトル鍵復号化部６５３は、利用者端末第二可搬媒体挿入処理部６５１からタイトル識別子ＴＬＩＤと暗号化タイトル鍵ＥＮＣＴＬＫａを取得する。そして、利用者端末記録部６４から個別鍵ＩＫａを取得する。その次に、個別鍵ＩＫａを基に暗号化タイトル鍵ＥＮＣＴＬＫａの復号化を行い、タイトル鍵ＴＬＫを取得する。最後に、タイトル識別子ＴＬＩＤとそのタイトル鍵ＴＬＫを利用者端末記録部６４へ記録する。終了する。（Ｓ６０７）
＜利用者端末６ａへ第一可搬媒体４を挿入した場合の動作＞
第一可搬媒体挿入処理部６５５は、第一可搬媒体アクセス部６２経由で利用者端末６ａに第一可搬媒体４が挿入されたことを検知する。（Ｓ６５１）
第一可搬媒体挿入処理部６５５は、第一可搬媒体アクセス部６２経由で第一可搬媒体４に記録されているタイトル識別子ＴＬＩＤを取得する。（Ｓ６５２）
利用者端末記録部６４にタイトル識別子ＴＬＩＤに対応するタイトル鍵ＴＬＫが記録されている場合、ステップＳ６５４へ進む。利用者端末記録部６４にタイトル識別子ＴＬＩＤに対応するタイトル鍵ＴＬＫが記録されていない場合、処理を終了する。（Ｓ６５３）
利用者端末記録部６４からタイトル鍵ＴＬＫを取得し、デスクランブル処理部６５６へ出力する。（Ｓ６５４）
デスクランブル処理部６５６は、第一可搬媒体挿入処理部６５５からタイトル鍵ＴＬＫを取得する。その後、第一可搬媒体アクセス部６２経由で第一可搬媒体４に記録されている暗号化コンテンツを逐次取得し、タイトル鍵ＴＬＫを基に暗号化コンテンツを逐次デスクランブルを行い、出力部６３経由で外部へ逐次出力する。全暗号化コンテンツのデスクランブルと外部出力が終了したら、処理を終了する。（Ｓ６５５）
以上が、クローン端末発見システム１の構成要素である利用者端末６ａの構成と動作である。なお、利用者端末６ａと他の利用者端末６ｂ～６ｎとの相違点は、利用者端末記録部６４において予めそれぞれ異なる利用者端末識別子ＴＭＩＤｂ～ＴＭＩＤｎと第一利用

者端末乱数ＴＭＲＮＤｌｂ～ＴＭＲＮＤｌｎと個別鍵ＩＫｂ～ＩＫｎを保持している点が異なる。

【００４９】

尚、利用者端末制御部の各機能ブロックは典型的には集積回路であるＬＳＩとして実現されていてもよい。これらは個別にｌチップ化されても良いし、一部又は全てを含むようにｌチップ化されても良い。

ここでは、ＬＳＩとしたが、集積度の違いにより、ＩＣ、システムＬＳＩ、スーパーＬＳＩ、ウルトラＬＳＩと呼称されることもある。

【００５０】

また、集積回路化の手法はＬＳＩに限るものではなく、専用回路又は汎用プロセサで実現してもよい。ＬＳＩ製造後に、プログラムすることが可能なＦＰＧＡ（Ｆｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ）や、ＬＳＩ内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサー を利用しても良い。

さらには、半導体技術の進歩又は派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適応等が可能性としてありえる。

【００５１】

＜実施形態１の効果＞

ここでは、利用者端末の一つ（ここでは６ａとする）が内部解析され、利用者端末６ａの端末情報として利用者端末識別子ＴＭＩＤａと個別鍵ＩＫａと第一利用者端末乱数ＴＭＲＮＤｌａが外部へ漏洩した場合を例に挙げ、本発明の実施形態１の効果を説明する。まず、その利用者端末６ａの端末情報が外部に漏洩した場合、その端末情報を保持する大量のクローン端末（ここではその一つを６ｘとする）が市場に出回る可能性がある。つまり、利用者端末６ａとクローン端末６ｘは同じ端末情報（利用者端末識別子ＴＭＩＤａと個別鍵ＩＫａと第一利用者端末乱数ＴＭＲＮＤｌａ）を保持していることとなる。ここでは、利用者端末６ａの利用者（利用者ａと呼ぶ）とクローン端末６ｘの利用者（利用者ｘと呼ぶ）は異なると想定し、また、利用者ａと利用者ｘはそれぞれ異なる第二可搬媒体５ａと５ｘを保持しているとする。まず一般的なシナリオとして、利用者端末６ａの利用者ａが小売店にコンテンツの入った第一可搬媒体４を購入しに行くとする。その場合、利用者ａの保持する第二可搬媒体５ａを小売店に設置されている情報収集サーバ３に挿入する。ここで、管理センタ２は、第二可搬媒体５ａに、暗号化されたタイトル鍵に加え、利用者端末識別子ＴＭＩＤａの利用者端末向けの新たな乱数として第二利用者端末乱数を書き込む。利用者ａはその第二可搬媒体５ａを利用者端末６ａに挿入し、利用者端末６ａが保持する第一利用者端末乱数の値を第二可搬媒体５ａに記録されている第二利用者端末乱数の値に更新する。そして、続いて利用者ａが別のコンテンツを購入する際に、同様に第二可搬媒体５ａを小売店に設置されている情報収集サーバ３に挿入する。その際、第二可搬媒体５ａには第一利用者端末乱数として新しい乱数の値が設定されている。それを受け取った管理センタ２は、利用者端末識別子ＴＭＩＤａに対応する利用者端末（６ａ）の第一利用者端末乱数が更新されたことを知る。その後、クローン端末６ｘの利用者ｘがコンテンツを購入しに小売店に行くとする。その際、利用者ｘは、同様に第二可搬媒体５ｘを小売店に設置されている情報収集サーバ３に挿入する。その際、その利用者ｘが保持する第二可搬媒体５ｘには、利用者端末識別子ＴＭＩＤａと、端末情報が漏洩した時点の古い第一利用者端末乱数が書き込まれている。よって、管理センタ２は、利用者端末識別子ＴＭＩＤａに対応する利用者端末（６ｘ）が、古い第一利用者端末乱数を保持していると認識する。しかし、管理センタ２は、利用者端末識別子ＴＭＩＤａに対応する利用者端末（６ａ）の第一利用者端末乱数が新たな乱数に更新されたと認識している。その結果から、同じ利用者端末識別子ＴＭＩＤａを保持する利用者端末が市場に二台以上存在すると判断する。そして、利用者端末識別子ＴＭＩＤａに対応する利用者端末にクローンが存在する旨、警告を表示する。このようにして、本発明の実施形態１では、利用者端末のクローンが存在することを効率的に発見、検知することが出来る。

【００５２】
また、クローン利用者端末の別の形として、利用者端末の一つ（ここでも６ａとする）が内部解析され、利用者端末６ａに関する端末情報（利用者端末識別子ＴＭＩＤａと個別鍵とＩＫａ第一利用者端末乱数ＴＭＲＮＤ１ａ）が外部へ漏洩した場合に、クローン検知を逃れる目的で、その利用者端末識別子（ＴＭＩＤａ）を違う偽の値（ここではＴＭＩＤｙとする）にしてクローン端末６ｙに埋め込む不正が考えられる。しかし、本発明の実施形態１では、管理センタ２は購入した暗号化コンテンツのタイトル鍵を、受け取った利用者端末識別子に対応する個別鍵で暗号化した暗号化タイトル鍵を提供するようにした。それにより、偽の利用者端末識別子ＴＭＩＤｙを管理センタ２に渡した場合、そのクローン端末６ｙが保持する個別鍵ＩＫａでは、受け取る暗号化タイトル鍵を復号化出来ないこととなる。つまり、クローン端末６ｙでは購入したコンテンツの出力が出来ないこととなる。これは、漏洩した利用者端末識別子を違う偽の値にして管理センタ２へ提供しても意味がないことに繋がる。よって、本発明の実施形態１では、漏洩した利用者端末識別子を偽造することの抑止力として効果的である。
【００５３】
＜実施形態１の変形例＞
上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において主な態様で実施し得るものである。以下のような場合も本発明に含まれる。
（１）本実施形態１では、第二可搬媒体が情報収集サーバに挿入される毎に、管理センタ２は新たな乱数を生成し、それを第二利用者端末乱数として第二可搬媒体に記録するようにして、利用者端末の乱数を毎回更新するようにしていたが、これに限るものではない。例えば、ある一定期間（例えば一ヶ月）に一回のみ乱数を更新するようにしてもよい。また、外部から乱数更新要求信号を受けた時にのみ、乱数を更新するようにしてもよい。また、ある一定回数（例えば１０回）コンテンツを購入する毎に、乱数を更新するようにしてもよい。これは、乱数を更新しない場合に、管理センタ２は新たな乱数を生成せず、第二利用者端末乱数を第二可搬媒体に記録しないようにすることで実現可能である。
【００５４】
（２）本実施形態１では、端末情報として乱数を用いていたが、該当端末を保持しない第三者ユーザによって推定できず、さらに、管理センタ２が把握可能な値であれさえすれば、乱数でなくてもよい。例えば、シリアル番号で０から一つずつカウントアップしていってもよい。また、管理センタ２が情報収集サーバからデータを受け取った時刻に関する情報でも良い。また、情報収集サーバ３へ第二可搬媒体が挿入された時刻に関する情報でも良い。また、情報収集サーバ３へ第二可搬媒体が挿入された延べ回数でも良い。また、対応する利用者端末で以前に外部へ出力したコンテンツタイトルの履歴に関する情報であってもよい。また、それらの値のハッシュ値であっても良い。
【００５５】
（３）本実施形態１では、端末情報として乱数を用いていたが、該当端末を保持しない第三者ユーザによって推定できず、さらに、各利用者端末が自動で更新される値であれさえすれば、乱数でなくてもよい。例えば、利用者端末に第二可搬媒体が最後に挿入された時刻情報でも良い。また、利用者端末に第二可搬媒体が挿入された延べ回数でも良い。この場合、管理センタ２は特に端末情報を更新する必要がなくなる。これにより、管理センタ２の手間を軽減することが可能となる。
【００５６】
（４）本実施形態１では、ユーザは第二可搬媒体を一つずつ保持している場合を例に説明を行ったが、これに限られるものではない。たとえば、一人のユーザが二枚以上の第二可搬媒体を保持していても良い。このような場合に、同じ利用者端末識別子を複数の第二可搬媒体が保持し、管理センタ２は、同じ利用者端末識別子を複数の第二可搬媒体経由で受け取る場合が考えられる。その際に、管理センタ２は、その利用者端末識別子に対応する第二利用者端末乱数を、その内の一つの第二可搬媒体にのみ書き込んでも良いし、一つ

の利用者端末識別子に対応する同じ第二利用者端末乱数を、複数の第二可搬媒体に書き込むようにしても良い。前者の場合、第二利用者端末乱数を書き込まれた第二可搬媒体をユーザが紛失した場合に、利用者端末の乱数を更新できないという欠点がある。一方、後者の場合、第二利用者端末乱数を書き込まれた第二可搬媒体をユーザが紛失した場合にでも、別の第二可搬媒体を用いて利用者端末の乱数を更新できるという利点がある。後者を実現するために、第二可搬媒体に記録する端末情報として乱数更新完了フラグを追加してもよい。乱数更新完了フラグは、第二可搬媒体に記録されている第二利用者端末乱数の値に、該当する利用者端末の第一利用者端末乱数の値の更新が完了した場合に、第二可搬媒体に書き込むフラグである。このようなフラグを追加することによって、一つの利用者端末識別子に対応する同じ第二利用者端末乱数を、複数の第二可搬媒体に書き込むようにして、その複数の第二可搬媒体を介して端末情報が管理センタ２へ提供されたとしても、乱数更新完了フラグが記録されている場合にのみ利用者端末の乱数更新が完了したと認識することが出来る。

【００５７】

（５）本実施形態１では、第二可搬媒体はＳＤカード等のポータブルメディアであったが、これに限るものではない。例えば、演算処理の可能なＩＣカードでも良い。その場合、例えば、第二可搬媒体は、暗号処理等で利用者端末を認証してから端末情報やタイトル鍵情報を提供するようにしてもよい。これにより、より安全なシステムを構築することが出来る。また、変形例（４）の乱数更新完了フラグをＩＣカード内で追加するようにしてもよい。これにより、不正な利用者端末が、第二可搬媒体に乱数更新完了フラグを立てないという不正を排除することが出来る。

【００５８】

（６）本実施形態１では、管理センタ２は、第二可搬媒体経由で端末情報を収集する見返りにタイトル鍵情報を提供していたが、これに限るものはない。例えば、管理センタ２は、管理センタ２は、第二可搬媒体経由で端末情報を収集するだけで、特に情報を提供しなくてもよい。また、管理センタ２は、第二可搬媒体経由で端末情報を収集する見返りに一定期間（例えば１ヶ月）有効なライセンスを利用者端末に提供し、そのライセンスをある一定期間毎に取得しないと、利用者端末が利用不可になるような仕組みを備えていてもよい。

【００５９】

（７）本実施形態１では、クローンを発見する対象は、コンテンツを出力する利用者端末であったが、本技術はこれに限るものではない。例えば、第二可搬媒体（例：ＳＤカード）でも良い。また、電車の定期券や回数券や乗車券、ＩＣカード、クレジットカード、キャッシュカード、デビットカード、電子マネー、電子チケット、電子パスポート（電子旅券）、入出門管理カード、運転免許書、住民基本台帳カード、携帯電話、ＰＤＡ、ＳＴＢ（セットトップボックス）、電子ブック、コンピュータ、ＩＣタグ、コンピュータソフトウエア、オンラインゲームのライセンスなどでもよい。この場合、クローンを発見する対象に、乱数を保持させることとなる。これにより、コンテンツを出力する利用者端末以外でも、クローンを発見することが出来る。

【００６０】

（８）本実施形態１では、暗号化方法は、秘密鍵暗号方式ＡＥＳを利用していたが、これに限るものではない。例えば、別の秘密鍵暗号方式（例えばＤＥＳ）でも良いし、公開鍵暗号（例えばＲＳＡ方式）でもよいし、別の暗号方式でもよい。

（９）本実施形態１では、管理センタ２が、同一の利用者端末識別子に対応する異なる二種類の第一利用者端末乱数を受け取った場合に、その利用者端末識別子に対応する利用者端末はクローンであると判断していたが、これに限るものではない。例えば、同一の利用者端末識別子に対応するある閾値（例えば３）以上の異なる第一利用者端末乱数を受け取った場合に、その利用者端末識別子に対応する利用者端末はクローンであると判断してもよい。これにより、クローンの誤検知の確率を少なくすることが出来る。また、これは、同じ利用者端末識別子を複数の利用者端末が共有するようなシステムにも適用出来る。

例えば、利用者端末識別子が、機種毎に共通な場合である。この場合、閾値としては、同じ利用者端末識別子を有する利用者端末の数以上に設定するようにする。このようにすることで、同じ利用者端末識別子を複数の利用者端末が共有するようなシステムであっても、クローンを検知することが出来る。

【００６１】

（１０）本実施形態１では、第二可搬媒体５ａ～５ｍは１３個であったが、これに限るものではない。例えば、１２個以下でもよいし、１４個以上であってもよい。また、利用者端末６ａ～６ｎは１４台であったが、これに限るものではない。例えば、１５台以上であっても良いし、１３台以下であっても良い。また、情報収集サーバ３の数は、１台以上であれば何台でも良い。また、第一可搬媒体４の数も、１個以上であれば何個でも良い。タイトル識別子及びタイトル鍵の種類も、１種類以上であれば何種類でも良い。

【００６２】

（１１）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしても良い。また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ―ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ　Ｄｉｓｃ）、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

【００６３】

（１２）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【産業上の利用可能性】

【００６４】

コンテンツを端末へ配布するシステムにおいて、端末のクローンが存在するか否か判断を行う必要が生じた場合に、特に有用である。

【図面の簡単な説明】

【００６５】

【図１】本発明の実施の形態１におけるクローン端末発見システム１の概要図

【図２】本発明の実施の形態１における第一可搬媒体４の構成例を示す図

【図３】本発明の実施の形態１における第二可搬媒体５ａの構成例を示す図

【図４】本発明の実施の形態１における管理センタ２の構成例を示す図

【図５】本発明の実施の形態１における管理センタ記録部２３の構成例を示す図

【図６】本発明の実施の形態１における管理センタ２の動作の一例を示す図

【図７】本発明の実施の形態１における情報収集サーバ３の構成例を示す図

【図８】本発明の実施の形態１における情報収集サーバ３の動作の一例を示す図

【図９】本発明の実施の形態１における利用者端末６ａの構成例を示す図

【図１０】本発明の実施の形態１における利用者端末記録部６４の構成例を示す図

【図１１】本発明の実施の形態１における利用者端末６ａにおいて第二可搬媒体５ａを挿入した際の動作の一例を示す図

【図１２】本発明の実施の形態１における利用者端末６ａにおいて第一可搬媒体４を挿入した際の動作の一例を示す図

【符号の説明】

【００６６】

１　通信路

２　管理センタ

２１　管理センタ送受信部

２２　管理センタ表示部

２３　管理センタ記録部

２４　管理センタ制御部

２４１　管理センタ受信処理部

２４２　端末情報確認部

２４３　端末情報生成部

２４４　タイトル鍵暗号化部

２４５　管理センタ送信データ生成部

２４６　管理センタ送信処理部

３　情報収集サーバ

３１　情報収集サーバ送受信部

３２　情報収集サーバ第二可搬媒体アクセス部

３３　外部入力部

３４　情報収集サーバ制御部

３４１　情報収集サーバ第二可搬媒体挿入処理部

３４２　タイトル情報取得部

３４３　情報収集サーバ送信データ生成部

３４４　情報収集サーバ送信処理部

３４５　情報収集サーバ受信処理部

３４６　第二可搬媒体データ書込部

４　第一可搬媒体

５ａ～５ｍ　第二可搬媒体

６ａ～６ｎ　利用者端末

６１　利用者端末第二可搬媒体アクセス部

６２　第一可搬媒体アクセス部

６３　出力部

６４　利用者端末記録部

６５　利用者端末制御部

６５１　利用者端末第二可搬媒体挿入処理部

６５２　端末情報書込部

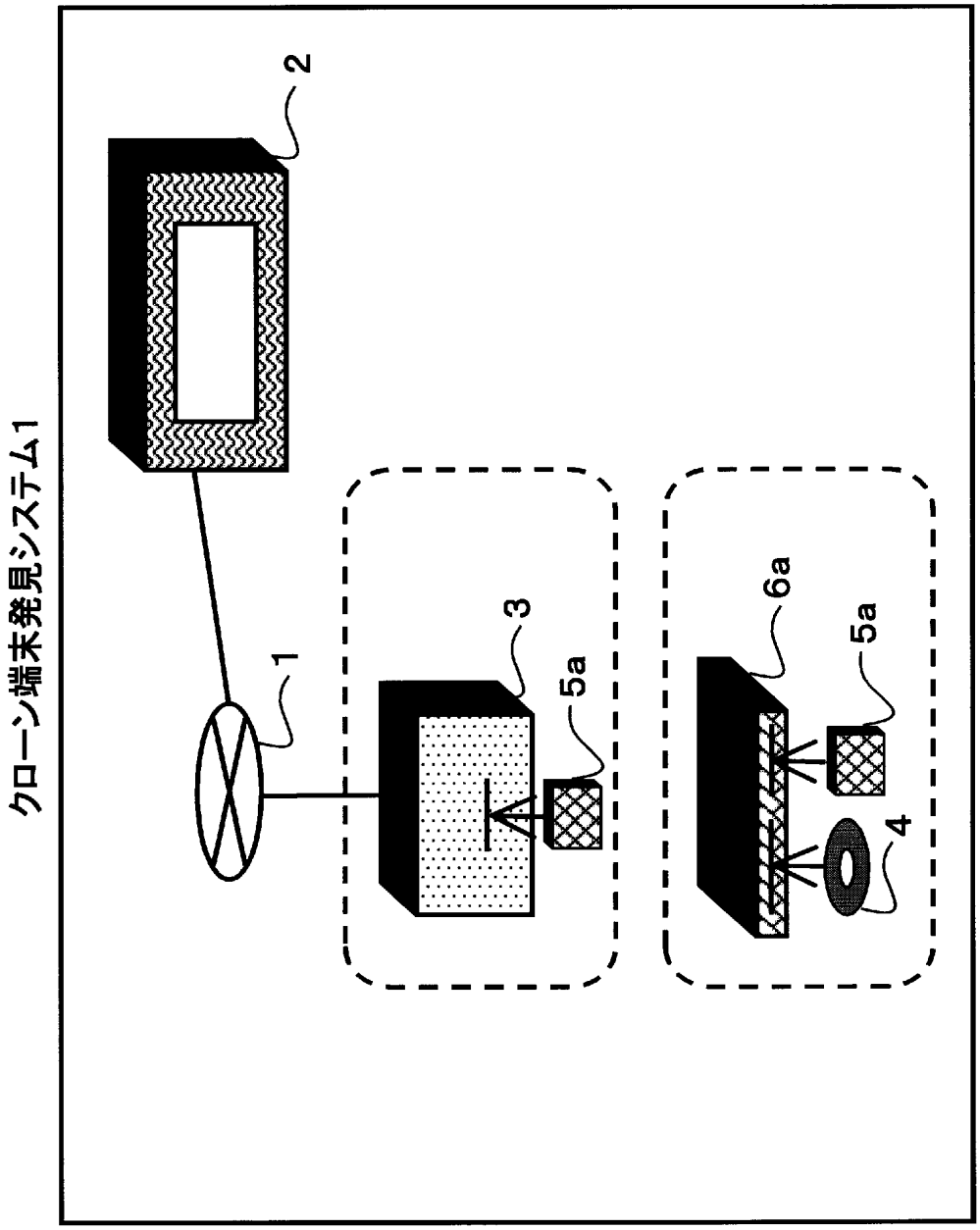
６５３　暗号化タイトル鍵復号化部

６５４　端末情報更新部

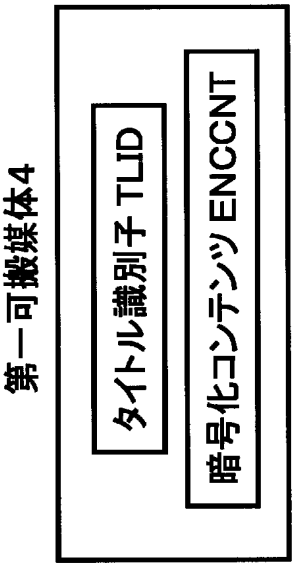
６５５　第一可搬媒体挿入処理部

６５６　デスクランブル部

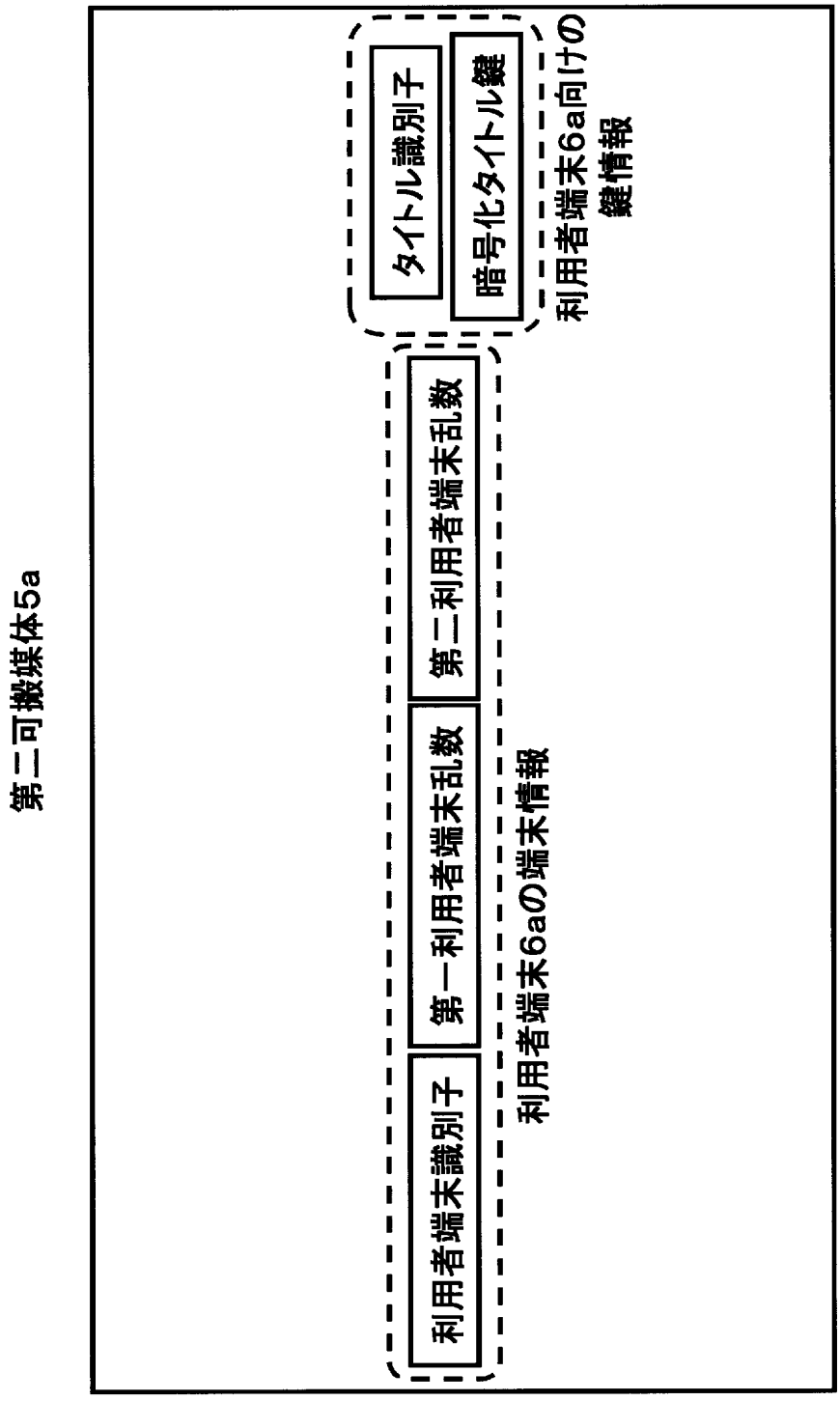
【書類名】図面
【図１】



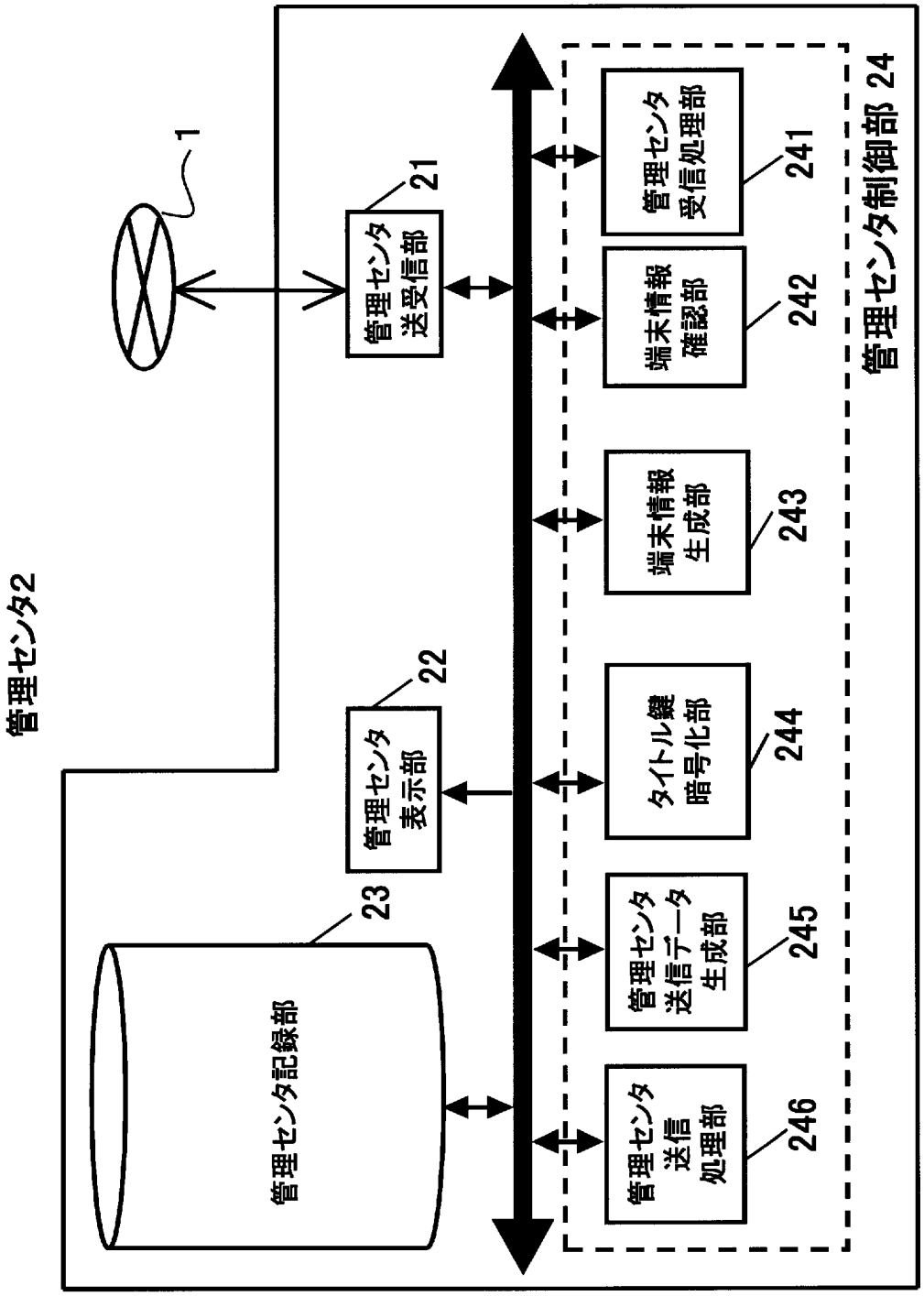
【図２】



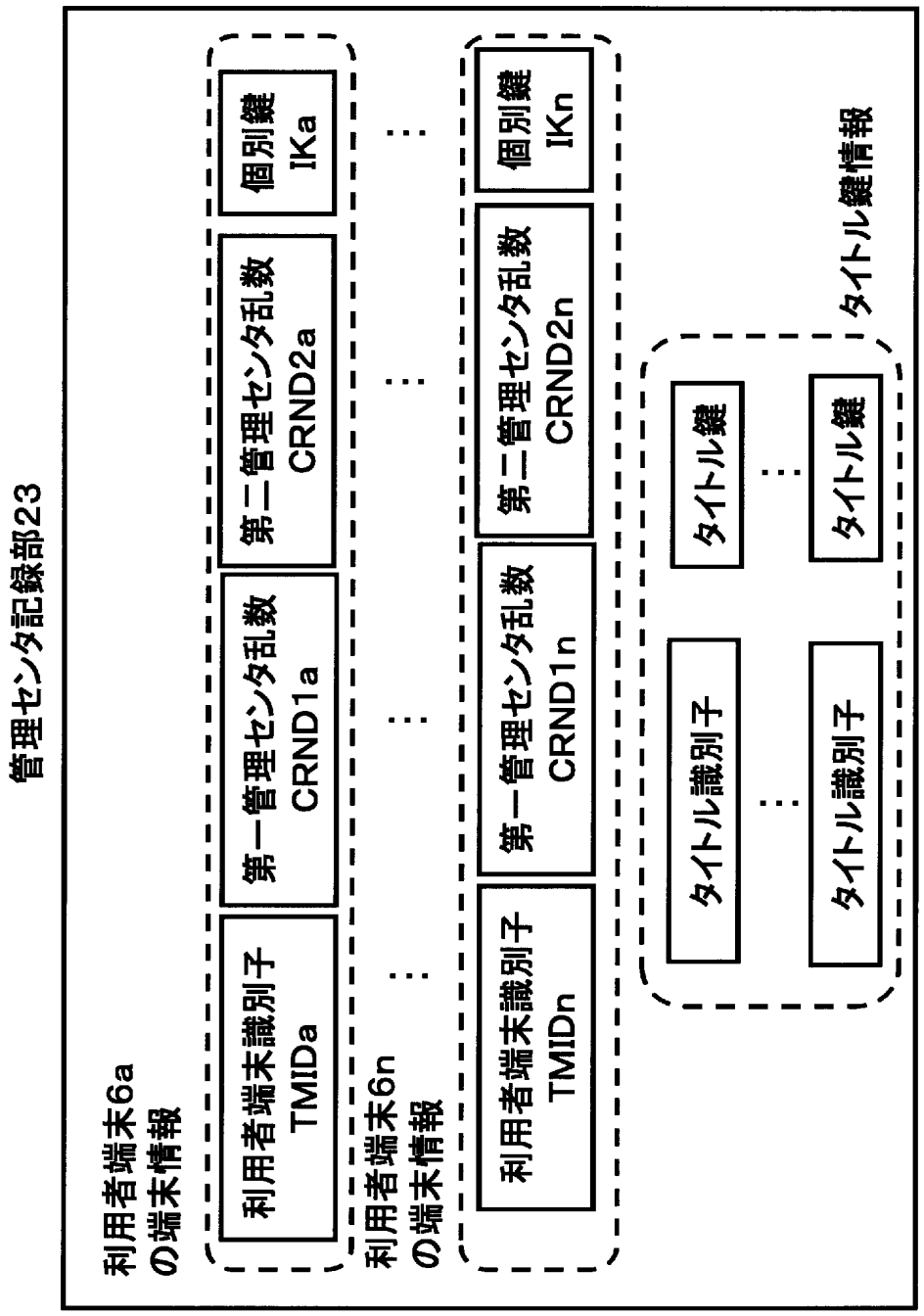
【図３】


第二可搬媒体5a
利用者端末識別子
第一利用者端末乱数
第二利用者端末乱数
利用者端末6aの端末情報
タイトル識別子
暗号化タイトル鍵
利用者端末6a向けの
鍵情報

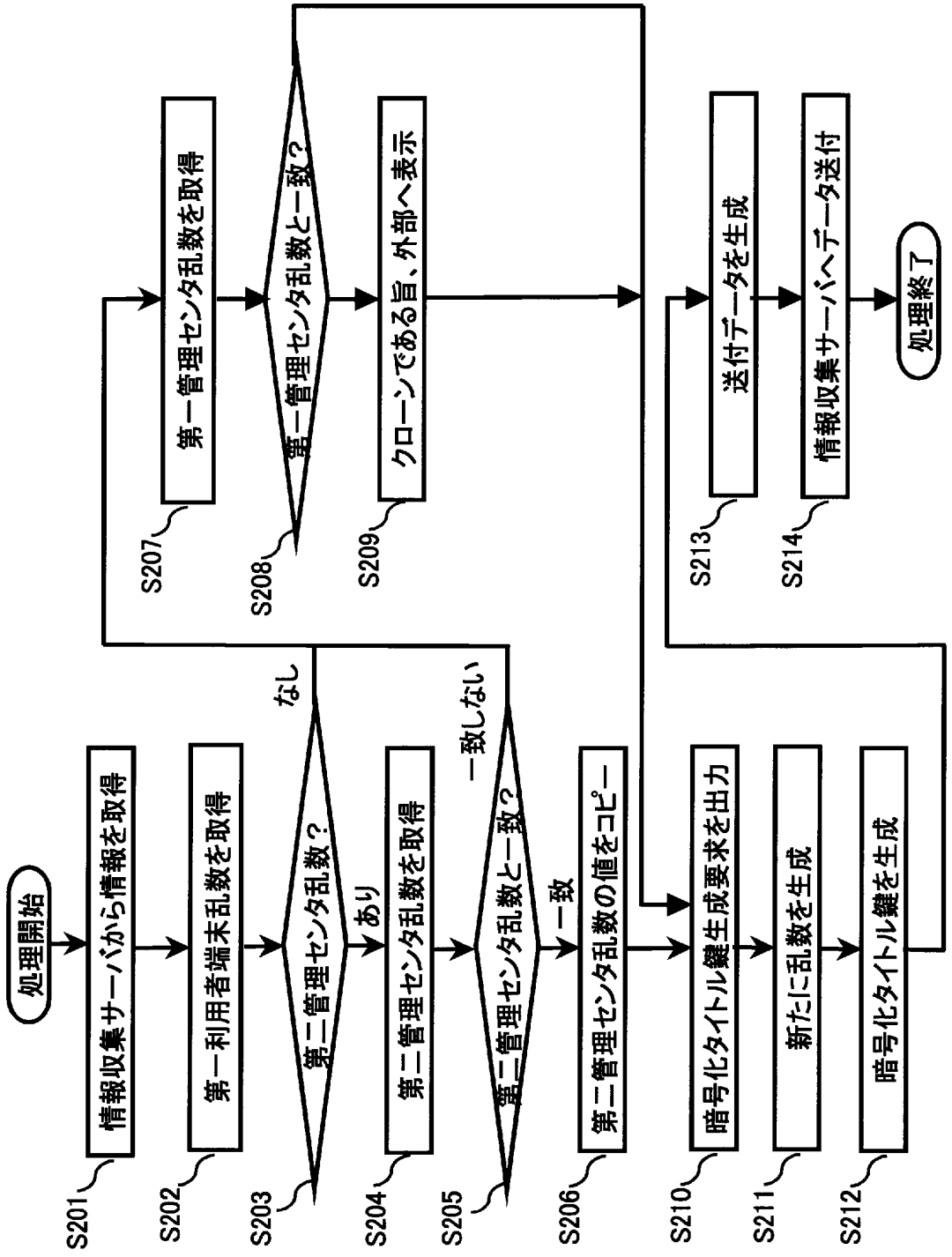
【図４】


管理センタ2
1
管理センタ送受信部
21
管理センタ表示部
22
管理センタ記録部
23
管理センタ制御部
24
管理センタ受信処理部
241
端末情報確認部
242
端末情報生成部
243
タイトル鍵暗号化部
244
管理センタ送信データ生成部
245
管理センタ送信処理部
246

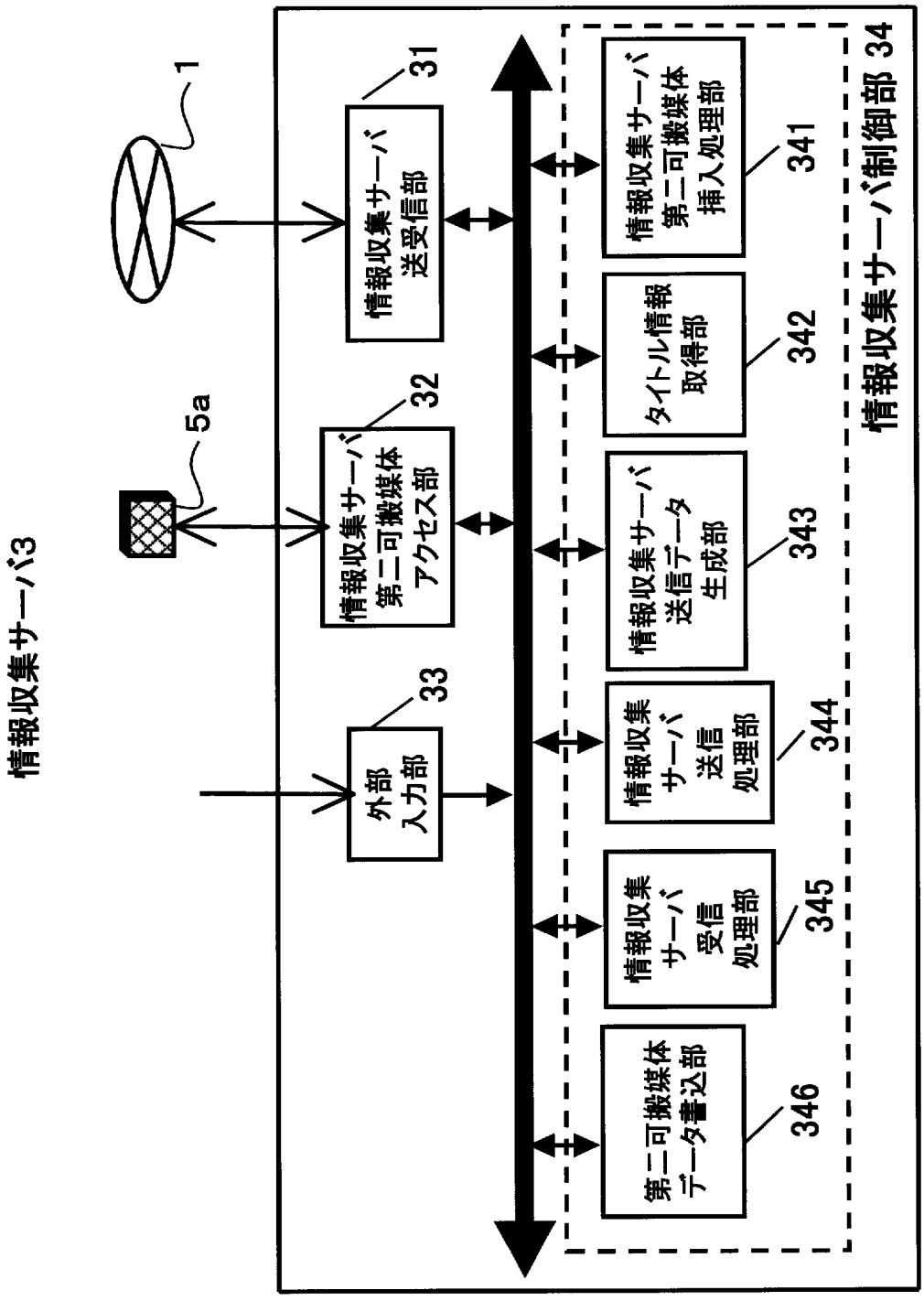
【図５】


管理センタ記録部23
利用者端末6aの端末情報
利用者端末識別子 TMIDa
第一管理センタ乱数 CRND1a
第二管理センタ乱数 CRND2a
個別鍵 IKa
利用者端末6nの端末情報
利用者端末識別子 TMIDn
第一管理センタ乱数 CRND1n
第二管理センタ乱数 CRND2n
個別鍵 IKn
タイトル識別子
タイトル鍵
タイトル識別子
タイトル鍵
タイトル鍵情報

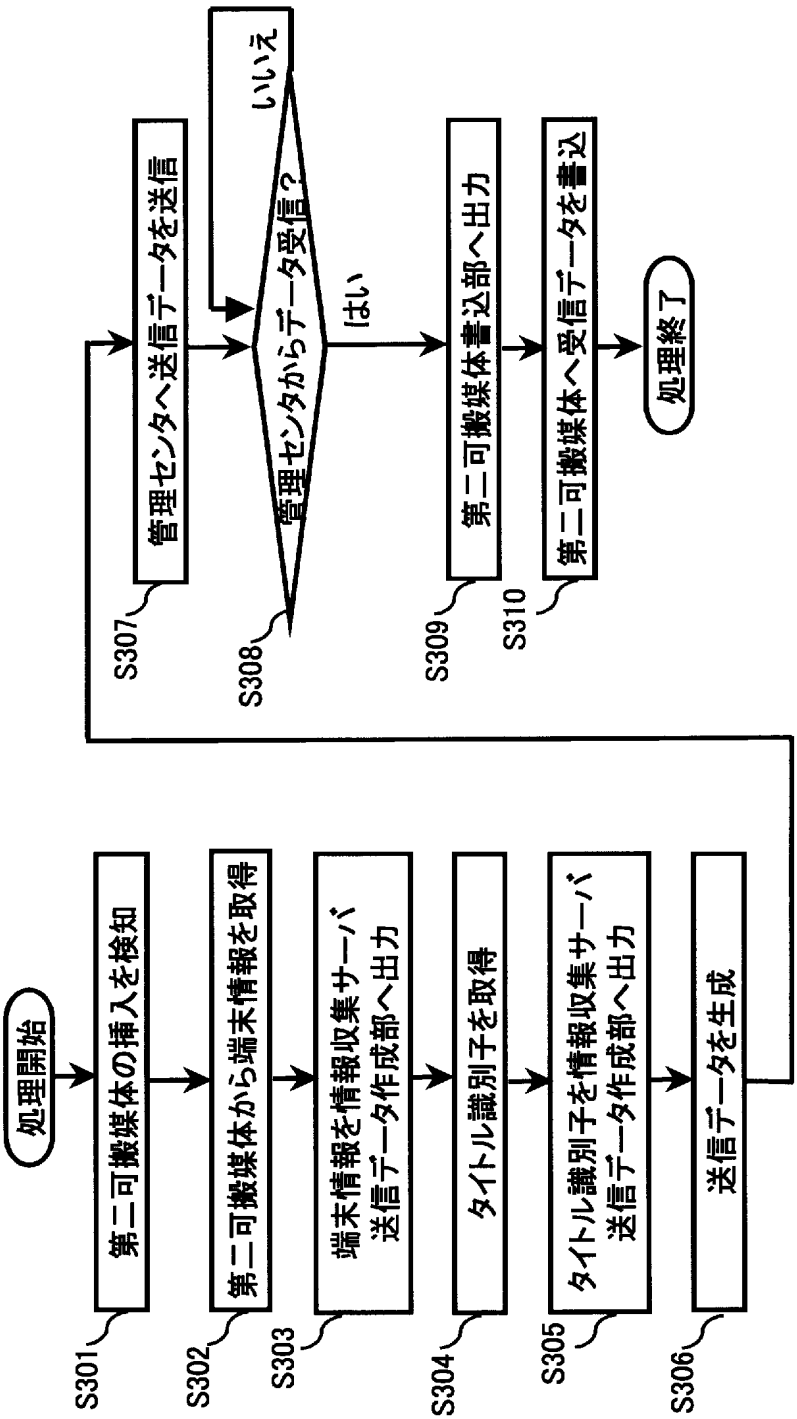
【図６】


処理開始
情報収集サーバから情報を取得
S201
第一利用者端末乱数を取得
S202
第二管理センタ乱数？
S203
なし
あり
第二管理センタ乱数を取得
S204
第二管理センタ乱数と一致？
S205
一致しない
一致
第二管理センタ乱数の値をコピー
S206
第一管理センタ乱数を取得
S207
第一管理センタ乱数と一致？
S208
クローンである旨、外部へ表示
S209
暗号化タイトル鍵生成要求を出力
S210
新たに乱数を生成
S211
暗号化タイトル鍵を生成
S212
送付データを生成
S213
情報収集サーバへデータ送付
S214
処理終了

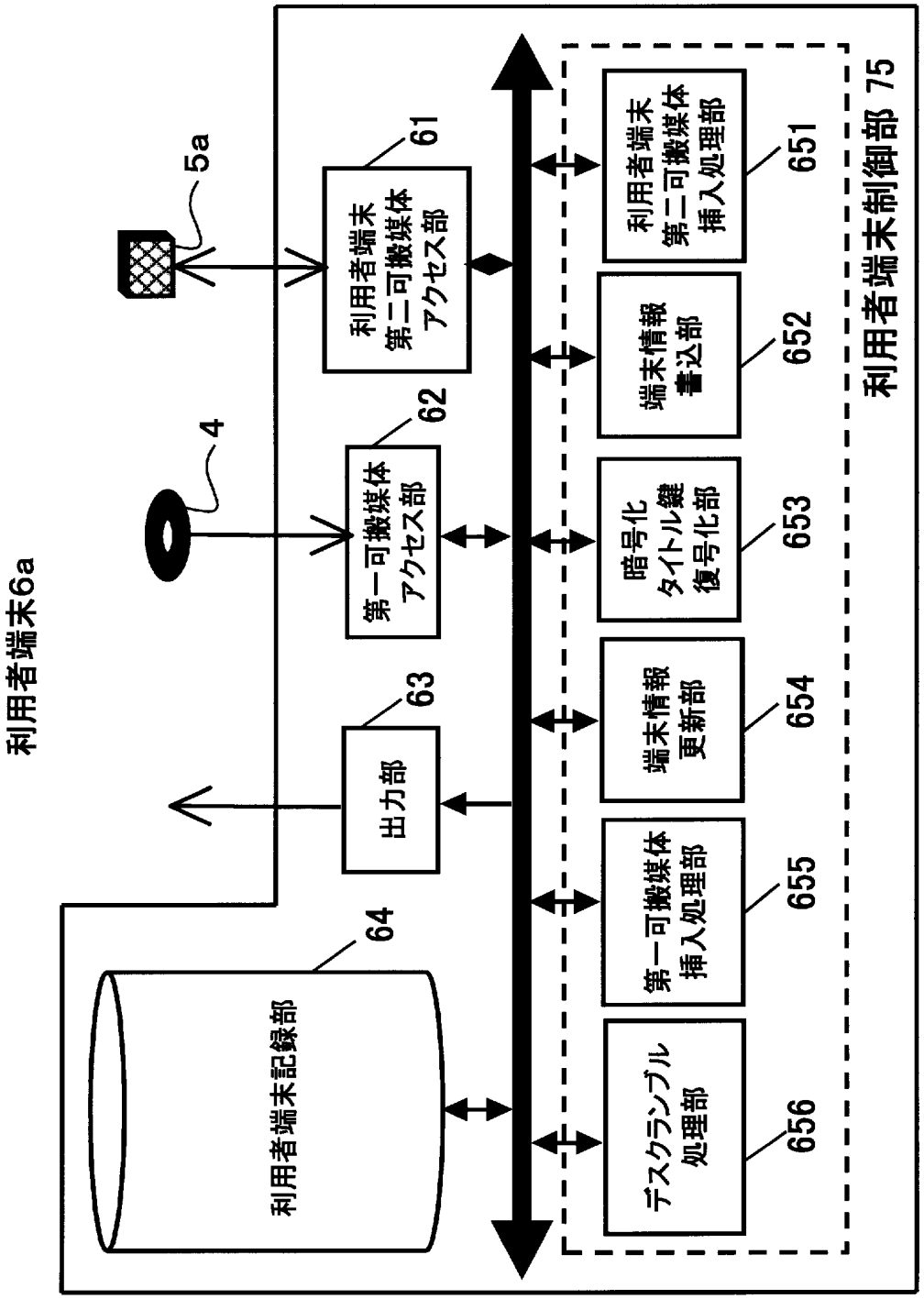
【図７】


情報収集サーバ3
1
5a
情報収集サーバ
送受信部
31
情報収集サーバ
第二可搬媒体
アクセス部
32
外部
入力部
33
情報収集サーバ制御部 34
情報収集サーバ
第二可搬媒体
挿入処理部
341
タイトル情報
取得部
342
情報収集サーバ
送信データ
生成部
343
情報収集
サーバ
送信
処理部
344
情報収集
サーバ
受信
処理部
345
第二可搬媒体
データ書込部
346

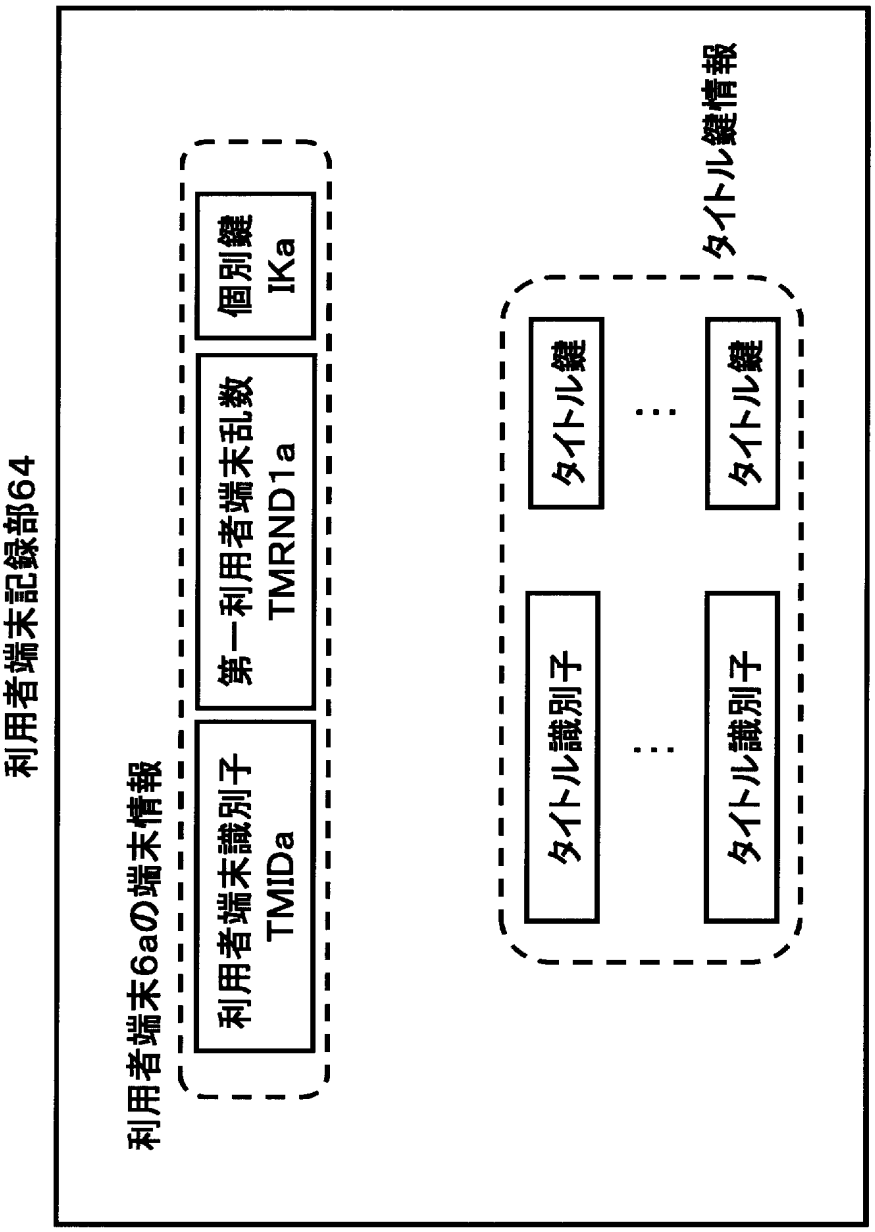
【図８】


処理開始
第二可搬媒体の挿入を検知
S301
第二可搬媒体から端末情報を取得
S302
端末情報を情報収集サーバ
送信データ作成部へ出力
S303
タイトル識別子を取得
S304
タイトル識別子を情報収集サーバ
送信データ作成部へ出力
S305
送信データを生成
S306
管理センタへ送信データを送信
S307
管理センタからデータ受信？
S308
いいえ
はい
第二可搬媒体書込部へ出力
S309
第二可搬媒体へ受信データを書込
S310
処理終了

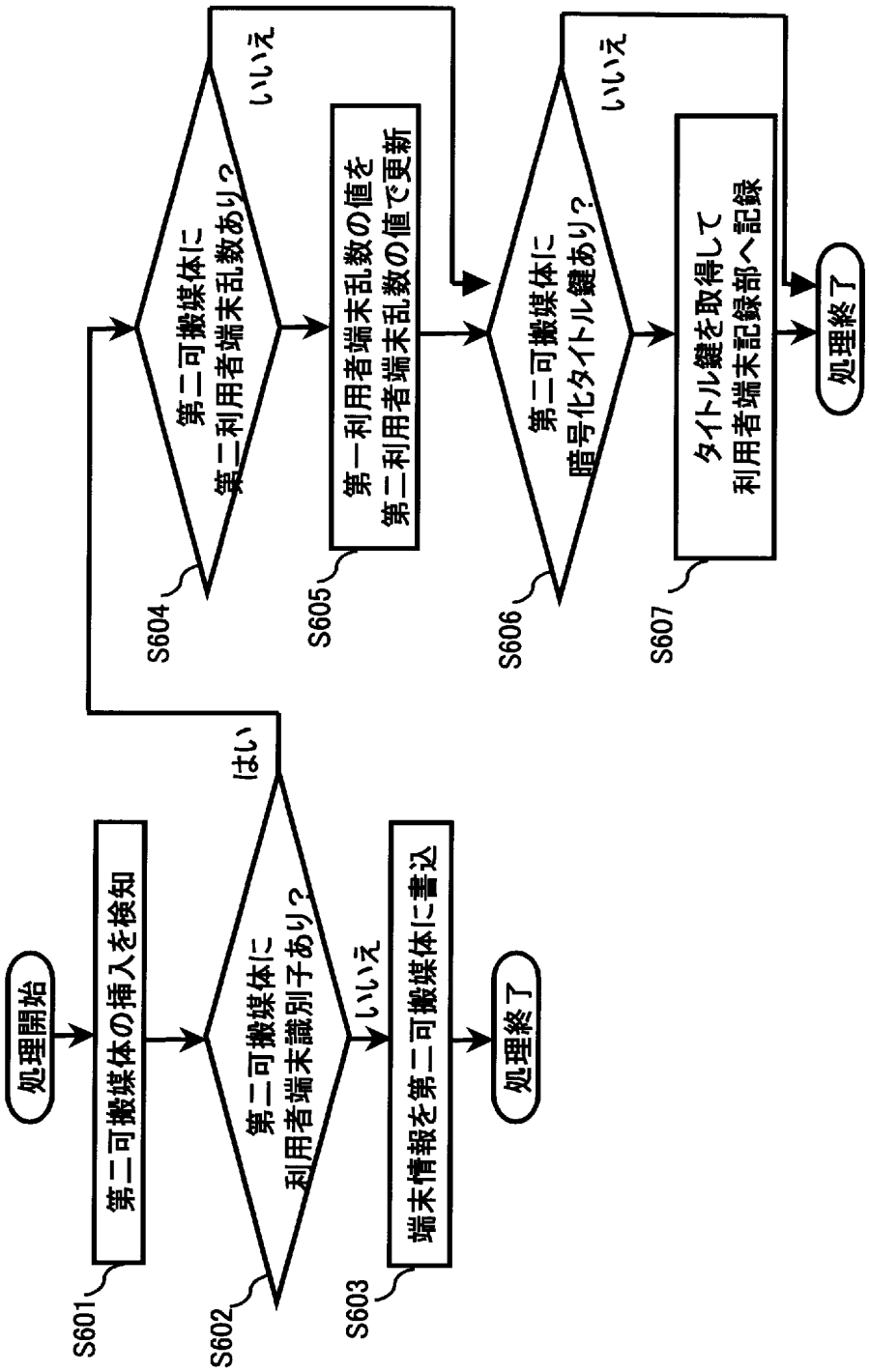
【図９】


利用者端末6a
5a
4
利用者端末記録部
64
出力部
63
第一可搬媒体
アクセス部
62
利用者端末
第二可搬媒体
アクセス部
61
利用者端末制御部 75
デスクランブル
処理部
656
第一可搬媒体
挿入処理部
655
端末情報
更新部
654
暗号化
タイトル鍵
復号化部
653
端末情報
書込部
652
利用者端末
第二可搬媒体
挿入処理部
651

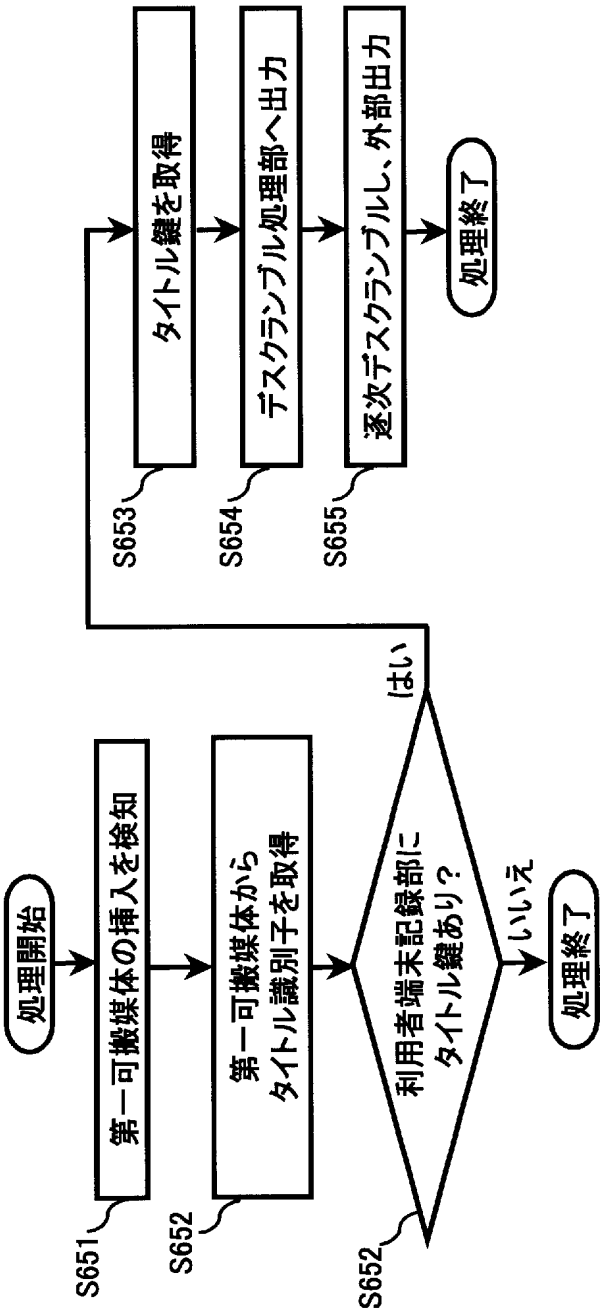
【図１０】


利用者端末記録部64
利用者端末6aの端末情報
利用者端末識別子
TMIDa
第一利用者端末乱数
TMRND1a
個別鍵
IKa
タイトル鍵情報
タイトル識別子
タイトル鍵
タイトル識別子
タイトル鍵

【図１１】


処理開始
第二可搬媒体の挿入を検知
S601
第二可搬媒体に
利用者端末識別子あり？
S602
はい
いいえ
端末情報を第二可搬媒体に書込
S603
処理終了
第二可搬媒体に
第二利用者端末乱数あり？
S604
いいえ
第一利用者端末乱数の値を
第二利用者端末乱数の値で更新
S605
第二可搬媒体に
暗号化タイトル鍵あり？
S606
いいえ
タイトル鍵を取得して
利用者端末記録部へ記録
S607
処理終了

【図１２】


処理開始
第一可搬媒体の挿入を検知
S651
第一可搬媒体から
タイトル識別子を取得
S652
利用者端末記録部に
タイトル鍵あり？
S652
はい
いいえ
処理終了
タイトル鍵を取得
S653
デスクランブル処理部へ出力
S654
逐次デスクランブルし、外部出力
S655
処理終了

【書類名】要約書
【要約】
【課題】外部に漏れた鍵を特定するためには、市場に大量流通したクローン端末／不正ソフトウェアを回収して、内部を解析することでしか特定できなかった
【解決手段】　本発明は、利用者端末のクローンを発見するクローン端末発見システムであって、前記クローン端末発見システムは、前記利用者端末にクローンが存在するか否かを判断する管理センタと、前記利用者端末に関する利用者端末端末情報を前記管理センタへ供給する一以上の情報収集サーバと、前記利用者端末端末情報を前記情報収集サーバへ供給する一以上の前記利用者端末と、から構成され、前記管理センタと前記情報収集サーバは通信路を介して通信可能であって、前記管理センタは、管理センタ端末情報を保持する管理センタ記録手段と、前記情報収集サーバから前記利用者端末端末情報を取得する手段と、前記管理センタ端末情報及び前記利用者端末端末情報を基に、前記利用者端末にクローンが存在するか否か判断する端末情報確認手段と、備え、前記情報収集サーバは、可搬媒体を介して、前記利用者端末から前記利用者端末端末情報を収集する情報収集サーバ可搬媒体挿入処理手段と、通信路を介して、前記前記利用者端末端末情報を前記管理センタへ供給する情報収集サーバ送信処理手段と、を備え、前記利用者端末は、前記利用者端末固有の前記利用者端末端末情報を保持する利用者端末記録手段と、前記可搬媒体を介して、前記利用者端末端末情報を前記情報収集サーバへ供給する可搬媒体データ書込手段と、を備えることを特徴とする。
【選択図】　図１

【書類名】　手続補正書
【整理番号】　2048160371
【提出日】　平成17年 2月23日
【あて先】　特許庁長官殿
【事件の表示】
　【出願番号】　特願2004-360436
【補正をする者】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【補正をする者】
　【識別番号】　504137912
　【氏名又は名称】　国立大学法人東京大学
【代理人】
　【識別番号】　100090446
　【弁理士】
　【氏名又は名称】　中島　司朗
【発送番号】　005515
【手数料補正】
　【補正対象書類名】　特許願
　【予納台帳番号】　014823
　【納付金額】　16,000円

【書類名】　手続補正書
【整理番号】　2048160371
【提出日】　平成17年 3月30日
【あて先】　特許庁長官　殿
【事件の表示】
　【出願番号】　特願2004-360436
【補正をする者】
　【識別番号】　000005821
　【住所又は居所】　大阪府門真市大字門真１００６番地
　【氏名又は名称】　松下電器産業株式会社
【補正をする者】
　【識別番号】　504137912
　【住所又は居所】　東京都文京区本郷７－３－１
　【氏名又は名称】　国立大学法人東京大学
【代理人】
　【識別番号】　100090446
　【住所又は居所】　大阪市北区豊崎３丁目２番１号淀川５番館６Ｆ
　【弁理士】
　【氏名又は名称】　中島　司朗
【手続補正1】
　【補正対象書類名】　特許願
　【補正対象項目名】　提出物件の目録
　【補正方法】　追加
　【補正の内容】
　　【提出物件の目録】
　　【物件名】　持分について証明する書面　1

【物件名】　　持分について証明する書面

東大—松下電器連携契約準拠

【添付書類】

持分証明書

平成１７年１月２８日

事件の表示　　平成１６年１２月１３日付特許願 2004-360436 号
整理番号　　(20481)H16-0371(乙内：依頼番号)
3004Z014-1（甲内：整理番号)

上記発明の特許を受ける権利の持分を国立大学法人 東京大学 50%、松下電器産業株式会社 50%と定めたことに相違ありません。

東京都文京区本郷七丁目三番一号
国立大学法人 東京大学
総長　佐々木　毅

大阪府門真市大字門真１００６番地
松下電器産業株式会社
取締役社長　　中村　邦夫

【書類名】　手続補正書
【整理番号】　2048160371
【提出日】　平成17年 8月 1日
【あて先】　特許庁長官　殿
【事件の表示】
　【出願番号】　特願2004-360436
【補正をする者】
　【識別番号】　000005821
　【住所又は居所】　大阪府門真市大字門真１００６番地
　【氏名又は名称】　松下電器産業株式会社
【補正をする者】
　【識別番号】　504137912
　【住所又は居所】　東京都文京区本郷７－３－１
　【氏名又は名称】　国立大学法人東京大学
【代理人】
　【識別番号】　100090446
　【住所又は居所】　大阪市北区豊崎３丁目２番１号淀川５番館６Ｆ
　【弁理士】
　【氏名又は名称】　中島　司朗
【発送番号】　052259
【手続補正1】
　【補正対象書類名】　手続補正書
　【補正対象書類提出日】　平成17年 3月30日
　【補正対象項目名】　持分について証明する書面
　【補正方法】　変更
　【補正の内容】
　　【提出物件の目録】
　　【物件名】　持分について証明する書面　1

【物件名】　持分について証明する書面

東大—松下電器連携契約準拠

【添付書類】

持分証明書

16 12 13
平成~~17~~年~~2~~月~~23~~日

事件の表示　平成１６年１２月１３日付特許願2004-360436号
整理番号　(20481)H16-0371(乙内：依頼番号)
3004Z014-1（甲内：整理番号）

上記発明の特許を受ける権利の持分を国立大学法人 東京大学50%、松下電器産業株式会社50%と定めたことに相違ありません。

東京都文京区本郷七丁目三番一号
国立大学法人 東京大学
総長　佐々木　毅

大阪府門真市大字門真１００６番地
松下電器産業株式会社
取締役社長　　中村　邦夫

出願人履歴

０００００５８２１
19900828
新規登録

大阪府門真市大字門真１００６番地
松下電器産業株式会社
５０４１３７９１２
20040406
新規登録

東京都文京区本郷７丁目３番１号
国立大学法人　東京大学